



The Effectiveness of Administrative Protection for Personal Data under the Newly Established E-Governance System in Iraq

Asst. Lect. Safa Abdul-Mahdi Jassim Ismail

University of Wasit / College of Arts

safa_lawyers95@gmail.com

Received Apr.15, 2026

Revised May 18, 2026

Accepted May29, 2026

Online Jul.1, 2026

ABSTRACT

One of the most prominent challenges facing these institutions is the adoption of e-government systems and the investment in modern technologies to enhance the quality of public services provided to beneficiaries. While this step may seem simple, it actually faces a series of challenges, particularly in the areas of administrative law and the protection of personal data. E-government is defined as the digital availability of government services and information via the internet, in addition to the use of other information technologies. However, these technologies are not without risks, as they facilitate access to citizens' personal data, raising legitimate questions about the extent of adherence to the principles and rules of administrative law and the protection of privacy. Therefore, administrative law emerges as a legal and methodological framework that seeks to regulate administrative conduct and the management of public affairs, and it acquires particular importance in preventing the abuse of citizens' rights and preserving their dignity. In this context, a set of regulations and laws has been adopted, both nationally and internationally, to establish mechanisms that guarantee the protection of individuals' privacy and ensure the integrity of personal data.

Keywords: Personal data, requirements, individuals, e-government system, privacy.

مدى فاعلية الحماية الإدارية للبيانات الشخصية في ظل نظام الحوكمة الإلكترونية المستحدث في العراق

م.م. صفا عبد المهدي جاسم اسماعيل

جامعة واسط / كلية الآداب

Email: safa_lawyers95@gmail.com

المخلص

أبرز التحديات التي تواجه هذه المؤسسات هو تبني أنظمة الحوكمة الإلكترونية واستثمار التقنيات الحديثة في سبيل تعزيز جودة الخدمات العامة المقدمة للمستفيدين. صحيح أن هذه الخطوة قد تبدو بسيطة، إلا أنها في الحقيقة تواجه سلسلة من التحديات، لا سيما في مجالات القانون الإداري وحماية البيانات الشخصية. وتعرف الحوكمة الإلكترونية على أنها الإتاحة الرقمية للخدمات والمعلومات الحكومية عبر الإنترنت، فضلا عن استخدام تقنيات المعلومات الأخرى. ومع ذلك، فإن هذه التقنيات لا تخلو من المخاطر، إذ تسهل الوصول إلى البيانات الشخصية للمواطنين، مما يؤثر تساؤلات مشروعة تخص مدى الالتزام بمبادئ وقواعد القانون الإداري وحماية الخصوصية. ولهذا يبرز القانون الإداري بوصفه إطارا قانونيا ومنهجيا يسعى إلى تنظيم السلوك الإداري وإدارة الشؤون العامة، ويكتسب أهمية خاصة في درء إساءة استخدام حقوق المواطنين والحفاظ على كرامتهم. وفي هذا السياق، تم اعتماد مجموعة من الأنظمة والقوانين، سواء على الصعيدين الوطني أو الدولي، بغية إنشاء آليات تضمن حماية خصوصية الأفراد وتؤمن سلامة البيانات الشخصية.

الكلمات المفتاحية: البيانات الشخصية، متطلبات، الأفراد، النظام الحكومي الإلكتروني، الخصوصية.



مقدمة:**أولاً: موضوع البحث**

لم تعد المعلومات قوة فحسب، وإنما أصبحت تجارة كبيرة، وفي السنوات الأخيرة كان قطاع الخدمات هو أسرع جوانب التجارة الدولية نمواً، إذ يصل إلى ما يزيد على ثلث التجارة العالمية، ولا يزال مستمراً في النمو، ومن الطبيعي معرفة أن اعتماد المجتمعات الصناعية الحديثة على حفظ المعلومات يعد سمة رئيسية لها، وبالطبع يؤدي استخدام أجهزة الكمبيوتر إلى كفاءة كبيرة وسرعة في جمع المعلومات وحفظها واستخدامها واسترجاعها ونقلها فإن الأعمال الروتينية للمؤسسات الحكومية والخاصة تتطلب تدفقاً مستمراً للمعلومات عنا من أجل الإدارة الفعالة لعدد لا يحصى من الخدمات التي تعد جزءاً لا يتجزأ من الحياة المعاصرة، وتقديم الخدمات الصحية وخدمات الضمان الاجتماعي والائتمان والتأمين واكتشاف الجرائم ومنعها؛ يفترض توافر كميات كبيرة من البيانات الشخصية، ومن ثم استعداد الأفراد لتقديمها، وعملية حوسبة هذه المعلومات التي غالباً ما تكون حساسة للغاية — تزيد من مخاطر سوء استخدامه وربما ضياعها، في الواقع، نتيجة للإهمال.

ثانياً: أهمية البحث

تبرز أهمية دراسة موضوع البحث من حماية البيانات تتصل بحق الخصوصية الذي يعد من أبرز الحقوق للصيقة بشخصية الإنسان، ولما كان الإنسان اجتماعياً بطبعه أخذ يحاول ان يعيش جانباً من حياته دون تدخل وبالقدر الذي لا يتركه بمعزل عن الجماعة، غير أنه في الوقت ذاته يجد نفسه في صراع مع داء تطفل الآخرين، الأمر الذي جعله من الضروري العمل جاهداً للمحافظة على أموره الخاصة وعدم جعلها عرضة أمام الغير، ومما لا شك فيه ان بعضهم يتساءل عن موضوع هذا الحق وخصوصاً لما بات من المؤكد ان هناك خلطاً واضحاً بين أنواع الحقوق عامة والصيقة بالشخصية بخاصة.

الأمر الذي في ضوئه آثرنا اختيار الموضوع ، فمن الناحية العملية هي ضرورة الإحاطة بتجريم المساس أو الاعتداء على هذا الحق بجميع صورته من جهة، ومن جهة أخرى اجتهادات القضاء بهذا المجال، أما من الناحية النظرية فتتمثل ابتداءً في فهم الخلفية الفلسفية والقانونية عما يعد خاصاً وما يعد من قبيل الحياة العامة، وبعبارة أخرى طبيعة هذا الحق ونطاقه، إذ إن نسبية هذا الحق جعلت منه محل خلاف فقهي، كما تبرز أهمية الدراسة من ناحية كثرة الأعمال الإدارية التي تتطلب الكشف عن الفرد عن بعض معلوماته كما هو الحال في التعاقدات الإدارية التي قد يضطر بعض الأحيان للكشف عنها للإدارة للتأكد من كفاءته المالية كما هو الحال في العقود التي تطلب فيها الإدارة التعاقد عبر المناقصات العامة، ولا تقف أهمية الدراسة لدى هذا الأمر بل تتعدى إلى أن الإدارة الإلكترونية فرضت ذاتها ضمن إدارة المرافق العامة الأمر الذي يحض المشرع على ابتداء نظام قادر على حماية كل ما يتم تداوله عبر الوسائل الإلكترونية من معلومات.

ثالثاً: إشكالية البحث

تبرز إشكالية الدراسة من ناحية التساؤل إلى أي مدى يمكن القول بوجود حماية إدارية فاعلة للبيانات الشخصية في ظل غياب تشريع عراقي شامل؟ وماهي آليات تفعيل هذه الحماية في سياق الحوكمة الإلكترونية؟

رابعاً: منهجية البحث

سوف نتبع في دراسة هذا الموضوع منهج الدراسة التحليلية للقانون العراقي مع الإشارة لبعض القوانين من مثل القانون المصري والفرنسي على سبيل الاستئناس مع الإشارة للتوجيه الأوربي بهذا الخصوص، ولا بد من الإشارة إلى أنه لانعدام وجود قواعد خاصة ضمن المنظومة الإدارية تقرر مسؤولية الإدارية عن حماية البيانات سوف نتناول هذه المسؤولية ضمن القانون المدني والقانون الجزائي العراقي.

خامساً: خطة البحث

ستكون دراسة موضوع البحث ضمن خطة بحثية مكونة من مبحثين، يكون المبحث الأول مخصصاً لموضوع الإطار المفاهيمي للبيانات الشخصية في نطاق القانون الإداري، ضمن مطلبين، ويكون المبحث الثاني عن موضوع المتطلبات الخاصة بحماية البيانات في القانون الإداري وصورها، ضمن مطلبين:

المبحث الأول

الإطار المفاهيمي للبيانات الشخصية في نطاق القانون الإداري

من المتفق عليه أن مستخدمي المواقع الإلكترونية في تزايد مستمر، وهذا ما يؤدي إلى تدفق هائل للبيانات المهددة بالانتهاك ولم تعد هذه المخاطر مقتصرة على منصات التواصل الاجتماعي، بل ظهرت مؤخراً العديد من غرف الدردشة والتطبيقات المتعددة، التي لا تقتصر على التفاعل بين الأصدقاء فحسب، بل بدأت أيضاً تتجلى مواقع جديدة تهدف إلى أغراض تجارية تستهدف البيانات الشخصية للمستخدمين بغية تقديم إعلانات تتماشى مع اهتماماتهم، وبينما يستمر المستخدمون في السير في هذا المجهول يتسرب إليهم جهل عميق، إذ يستخدمون هذه المنصات دون وعي تام لطبيعتها، مما يقتضي تسليط الضوء على ما تمتاز به من صفات تميزها عن سواها (العومان، 2022، 25)، وفي قبيل هذا الأمر سنحاول ضمن هذا المبحث بيان الإطار المفاهيمي للبيانات الشخصية في نطاق القانون الإداري، ضمن مطلبين:

المطلب الأول

التعريف بالبيانات الشخصية

في عصرنا الحاضر تتدفق البيانات بوتائر متسارعة، تتراد يومًا بعد يوم، متأثرة بكثرة المواقع والتطبيقات المتنوعة وهذه البيانات، بذاتها، تحمل طابعًا شخصيًا بامتياز إذ تمس حياة الأفراد الخاصة وتخصهم على نحو مباشر، وتجدر الإشارة إلى أن تبادل هذه البيانات لا يعرف حدودًا جغرافية، بل يتجاوز كل الأطر ليشمل أرجاء المعمورة وهذا يؤد حالة من القلق، إذ يصعب السيطرة عليها وحفظها، ولأهمية البيانات الشخصية وما يتعلق بها من خصائص تميزها ضمن نطاق القانون الإداري سنحاول ضمن هذا المطلب بيان المفهوم الخاص بها، وما يخصها من خصائص ضمن فرعين كما يأتي:

الفرع الأول

تعريف البيانات الشخصية

عند إمعان النظر في تعريفات البيانات الشخصية في غالبية الدول العربية، نجد أنها تشير إلى تلك البيانات القادرة على التعريف بالشخص وتمييزه عن غيره، إذ تتمثل السمة الأبرز في ارتباطها بالأفراد الطبيعيين، أما تعريف البيانات ضمن الفقه الغربي فنلتزم منه أن هناك حماية مقررّة للأشخاص الأحياء فقط، مما يعني أن التشريعات العربية تبرز تفوقًا ملحوظًا، إذ أكدت على حماية الشخص سواء كان حيًا أو ميتًا، تكريمًا لمبدأ الكرامة الإنسانية، إذ لا ينبغي أن يتحقق انتهاك خصوصية الفرد حتى بعد رحيله عن هذه الدنيا، بينما تقتصر التشريعات الغربية على ضرورة رفع الحماية بموت الشخص، فضلًا عن ذلك أن البيانات المخفاة تلك التي لا تدلّ أو يُستدل منها على شخص معين لا تتمتع بحق الخصوصية؛ إذ إن المجهول ليس له خصوصية، فتلك البيانات لا تُعد ذات طابع شخصي ما لم تكن مباشرة كاسم المستخدم ولقبه، أو غير مباشرة كالبريد الإلكتروني وكلمة المرور (قارة، 2007، 89).

لكن في ضمن بعض التشريعات كالتشريع المصري يعد هذا المصطلح (البيانات) من المفاهيم الحديثة نسبيًا في السياق القانوني المصري، إذ يُعتبر ركيزة أساسية من ركائز الحق في الخصوصية (راشد، 2019، 206)، وعلى الرغم من حداثة هذا المصطلح في البيئة القانونية ضمن التشريع العراقي ولاسيما مع انتشار أساليب الدعاية والإعلان الرقمي ضمن البيئة التجاري (صايل، 2025، 429، <https://DOI.org/10.31185/lark.4161>)، إلا أن أهمية البيانات الشخصية وحمايتها القانونية قد برزت بشكل مُلفت على الساحة العالمية إذ إن حجم تداول البيانات والمعلومات عبر منصات التواصل الاجتماعي والمواقع الحكومية والخاصة قد بلغ مستويات لم يسبق لها مثيل، فقد أصبحت هذه المواقع تعتمد بشكل محوري على البيانات الشخصية مما أفضى بدوره إلى تصاعد

التحديات الموجهة لهذه البيانات نتيجة للممارسات الحديثة التي تُستغل فيها لأغراض سياسية أو تجارية أو غير ذلك (مشعل، 2017، 34).

وقد عرّف المشرع المصري البيانات الشخصية بأنها: "أي معلومات تتعلق بشخص طبيعي مُحدد، أو يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين هذه البيانات وأي معلومات أخرى، مثل الاسم أو الصوت أو الصورة أو رقم تعريفه أو محدد للهوية على الإنترنت، وصولاً إلى أي بيانات يمكن أن تُحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية"، كما توجد بيانات تُصنّف على أنها حساسة وهي تلك التي تكشف عن الصحة النفسية أو العقلية أو البدنية أو الجينية، بالإضافة إلى القياسات الحيوية والبيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الوضع الأمني، ولا يُمكن إغفال أن بيانات الأطفال تُعتبر أيضاً من بيانات الحساسية الخاصة (مشعل، 2017، 35).

وبذلك قد وضع المشرع المصري إطاراً واضحاً لنطاق البيانات الشخصية التي تُعالج إلكترونياً وتستحق الحماية. ويظهر من التعريفات السابقة أن البيانات الشخصية تشمل كل المعلومات الخاصة بالشخص الطبيعي، والتي إذا تم الاطلاع عليها يُستدل منها على هوية صاحبها دون حاجة إلى وسائل إضافية. مثلما أورد المشرع أمثلة على هذه البيانات الشخصية، من مثل اسم الفرد، صوته، صورته، أو رقمه القومي أو التأميني، فضلاً عما يحدد هويته على الإنترنت من مثل حساباته على منصات التواصل الاجتماعي مثل فيسبوك وتويتر وإنستجرام وغيرها ولاسيما بعد ظهور الثورة الرقمية ضمن المجتمعات ومدى تأثير أفراد المجتمع بهذا التحول الرقمي (جمعة، 2022، 827، <https://DOI.org/10.31185/lark.Vol4.Iss47.2436>)، ولا تقتصر البيانات الشخصية على ذلك، بل تشمل أيضاً بيانات الهوية الصحية والنفسية والاقتصادية والثقافية والاجتماعية، وغيرها الكثير (علي، 2022، 14).

إن المشرع العراقي لم يقدم تعريفاً شاملاً للبيانات الشخصية بمفهومها العام مع أهمية ذكر هذا التعريف لما له من تداعيات تحديد هذا المفهوم على وجه الدقة وعدم تركه للاجتهادات والآراء التي قد تختلف في نظرتها بين ما يعد من قبيل البيانات وما يتطلب من حماية لها وما بين ما يعده مجرد معلومات شخصية ليس إلا، فالمشرع العراقي عرّف عن تحديد ماهية البيانات بالرغم من اتساع مدلولها وسرعة تطورها في عصر المعلومات، فتجده أحياناً يحدد بعض أشكالها، وأحياناً أخرى يشير إليها في نصوص متفرقة دون أن يضع لها تعريفاً دقيقاً مما يجعل موقفه من تصنيف تلك البيانات غامضاً، فضلاً عن ذلك لم يضع المشرع تنظيمًا مُحكمًا لأساليب معالجتها أو لتنظيمها أو لنشرها عبر الفضاء الإلكتروني، ويعود هذا الخلط في المفاهيم إلى التداخل بين البيانات الشخصية وحق الخصوصية الذي تم تضمينه في نصوص دستورية، حيث تنص المادة 17 على أن: "لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والأداب العامة" (دستور جمهورية العراق، 2005)، كما أكد المشرع في المادة 38 من الدستور على حرية التعبير عن الرأي، إذ ينص على أن: "تكفل الدولة، وبما لا يخل بالنظام العام والأداب: أولاً:- حرية التعبير عن الرأي بكل الوسائل. ثانياً:- حرية الصحافة والطباعة والاعلان والاعلام والنشر. ثالثاً:- حرية الاجتماع والتظاهر السلمي، وتنظم بقانون". كما تنص في المادة (40) على حرية التواصل والمراسلات: "حرية الاتصالات والمراسلات البريدية والبرقية والهاتفية والإلكترونية وغيرها مكفولة، ولا يجوز مراقبتها أو التنصت عليها، أو الكشف عنها، الا لضرورة قانونية وأمنية، وبقرار قضائي" (دستور جمهورية العراق، 2005)، ومن جهة أخرى أكدت المادة (46) على الحماية الدستورية لهذه الحقوق إذ تنص: "لا يكون تقييد ممارسة أي من الحقوق والحريات الواردة في هذا الدستور أو تحديدها الا بقانون أو بناءً عليه، على ألا يمس ذلك التحديد والتقييد جوهر الحق أو الحرية"، وعند صدور قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012 لم يحدد المشرع تعريفاً للبيانات الشخصية، ولكنه عرف المعلومات بأنها: "البيانات والنصوص والصور والأشكال والأصوات والرموز وما شابه ذلك التي تُنشأ أو تُدمج أو تُحزن أو تُعالج أو تُرسل أو تُستلم بالوسائل الإلكترونية" (قانون التوقيع الإلكتروني والمعاملات الإلكترونية، 2012).

وعليه فإن موقف المشرع العراقي في هذا السياق اقتصر على حصر صور وأنواع المعلومات، دون معالجة شاملة لما يتعلق بالبيانات الشخصية التي تُنتج وتُعالج وتُنشر بطرق إلكترونية ونجمل من ذلك أن المشرع العراقي لم يتبع سياسة تشريعية واضحة المعالم فيما يتعلق بتعريف البيانات الشخصية، إذ تجده أحياناً يتجاهلها وأحياناً أخرى يضع تعريفات لبعض صورها بالنظر إلى التشريع المصري، نرى أنه يظهر بوضوح أكثر مما فعل المشرع العراقي في تعريف البيانات الشخصية، فقد ورد ذلك في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، إذ عُرفت البيانات الشخصية بالعبارة التالية: "أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى" (قانون مكافحة جرائم تقنية المعلومات المصري، 2018).

وعندما صدر قانون حماية البيانات الشخصية المصري رقم 151 الذي نُشر في الجريدة الرسمية بالعدد 28 مكرر (هـ) بتاريخ 15 يوليو سنة 2020، فقد وُضع تعريف محدد لتلك البيانات في المادة الأولى من القانون فقد نصت على أن: "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر من طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريف، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية"، ومن خلال هذا التعريف يتبين لنا أن المشرع المصري قد أدرج جميع البيانات الشخصية تحت هذا الوصف مُشيراً إليها على سبيل المثال، مما يعني أن أيّاً من البيانات المذكورة يعد بياناً شخصياً.

أما المشرع الفرنسي فقد عرّف البيانات الشخصية بأنها: "أي معلومات تتعلق بشخص طبيعي تُعتبر بياناً شخصياً إذا كانت تتعلق بتحديد هويته أو يمكن من خلالها التعرف عليه بصورة مباشرة أو غير مباشرة، سواء كان ذلك بالاستناد إلى رقم هويته أو أي من المعلومات المرتبطة به" (قانون حماية البيانات الشخصية الفرنسي، 2004)، وعلى النحو ذاته توصل النظام الأوروبي العام لحماية البيانات الشخصية، المعروف باسم اللائحة رقم 679 لعام 2016 بتعريف تلك البيانات بأنها: "أي معلومات تتعلق بشخص طبيعي مخصص أو قابل للتحديد، إذ يمكن التعرف على هذا الشخص بشكل مباشر أو غير مباشر من خلال الرجوع إلى معرف معين، مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف عبر الإنترنت، أو من خلال مجموعة من العوامل المحددة التي تتعلق بخصائصه الفيزيائية أو الفيزيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية، بناءً على ما سبق يمكن القول إن البيانات الشخصية تتمثل في أي معلومات تعكس شخصية الفرد، مثل صورته أو بصماته، وتستند إلى صفاته الجسدية أو السلوكية أو الاجتماعية أو الاقتصادية، مما يتيح التعرف على هويته، وتتضمن هذه المعلومات أيضاً أي بيانات تتعلق بالشخص بطرق غير مباشرة، وبالتالي تُعتبر تلك المعلومات معياراً يحدد ما إذا كانت تحمل الطابع الشخصي، وعند تحقق هذا الشرط، تُصنف على أنها بيانات شخصية تستحق الحماية القانونية (التهامي، 2014، 5)، ومن الجدير بالذكر أن الحماية القانونية للبيانات الشخصية تقتصر على ما يتعلق بالشخص الطبيعي فحسب، إذ إنها تستثني الأشخاص المعنويين من نطاق هذه الحماية وقد عزز الفقه هذه الفكرة بالقول إن المشرع يهدف إلى حماية الحقوق اللازمة للشخص الطبيعي والتي لا تتوفر في الشخص المعنوي، وتُحمى البيانات الشخصية وفقاً للأسس العامة للمسؤولية المدنية (الأهواني، 1990، 20).

الفرع الثاني

خصائص البيانات الشخصية

بعد أن عرضنا في الفقرة السابقة تعريف البيانات الشخصية عبر الإنترنت، نعتزم في هذه الفقرة استكشاف الخصائص التي تتسم بها هذه البيانات، وذلك على النحو الآتي:

أولاً: ملازمتها للشخص: تُفهم هذه الخاصية في أن الحق في البيانات الشخصية لا يمارس إلا من قبل صاحبها، فهو الفرد الوحيد القادر على ممارسة هذا الحق، إذ يعد هذا الحق جزءاً لا يتجزأ من كينونة الإنسان، ومع ذلك يمكن للوكيل ذي الأهلية الكاملة أن يتولى الدعوى المتعلقة بالاعتداء على حق الخصوصية، بشرط أن تكون الوكالة واضحة وجلية، في هذا السياق يمكننا تحديد الوجود

الشخصي للإنسان بعنصرين: الأول طبيعي يتمثل في الجوانب العضوية والنفسية والعقلية، والثاني قانوني يظهر في الحقوق المرتبطة بالشخصية التي يقرها القانون، كحق الاسم والصورة والشرف والاعتبار وحرمة البيانات الشخصية (بو جمعة، 2012، 54).

ثانياً: **عدم كونها مالاً**: تعني هذه الخصيصة أن الحقوق التي تتعلق بالبيانات الشخصية ليست حقوقاً مالية، بل حقوق غير مالية تتعلق بالعناصر المكونة للشخصية الإنسانية، وهذه الحقوق مرتبطة ارتباطاً وثيقاً بكينونة الفرد مما يعني أن الحق في حرمة البيانات الشخصية يظل ملازماً لصفة الإنسان (شرف الدين، 2002، 189).

ثالثاً: **عدم قابليتها للتصرف**: تجدر الإشارة إلى أن هذا الحق لا يمكن التنازل عنه، فإذا قام أحدهم بالتنازل عن خصوصيته لوسائل الإعلام فهذا يعني انتهاك حريته الفردية، وهو أمر غير مقبول، فمن الممكن أن يتنازل الفرد عن القدرة على العمل، ولكن لا يمكن أن يتخلى الكاتب عن حقوقه في إنتاجه الفكري المستقبلي، كما لا يجوز التنازل عن الحق في البيانات الشخصية. وأيضاً يعد أي تنازل مؤقت مدته محددة باطلاً تماماً، كما هو الحال بالنسبة للتنازل المطلق ولا يمكن أن تُعد البيانات الشخصية موضوعاً للبيع أو الهبة أو الوصية، ومن ثم لا يمكن تصور تغيير صاحب الحق في هذه البيانات، كما أن الشخص لا يستطيع الخروج عن نطاق الحماية القانونية المقررة لحياته الخاصة عبر التصرف في هذا الحق (شرف الدين، 2002، 191).

رابعاً: **عدم خضوعها للتقادم**: يبقى الحق في حرمة الحياة الخاصة الذي يتضمن البيانات الشخصية قائماً دون أن يتأثر بالتقادم، فيظل للإنسان هذا الحق مهما طالت مدة عدم استخدامه له، وكذلك فهو لا يدخل ضمن الذمة المالية مما يجعله خارج دائرة التعامل. ومن الجدير بالذكر أن هناك فرقاً يميز بين الحق في الخصوصية والادعاءات القانونية المتصلة بالاعتداء على هذه البيانات أو دعاوى التعويض عن الأضرار الناتجة عن هذا التجاوز، فبينما يبقى الحق في البيانات الشخصية غير قابل للتقادم، فإن هذا لا يعني أن الدعاوى المتعلقة بالاعتداء عليها كذلك (بو جمعة، 2012، 55).

خامساً: **عدم انتقالها بالميراث**: بصفة عامة فإنّ الحقوق المرتبطة بالشخصية لا تنتقل بعد وفاة صاحبها حيث إن هذه الحقوق ملازمة لذاته، وعندما تنتضي هذه الشخصية فمن المنطقي أن تنتهي الحقوق التي ترتبط بها (بن عاشور، 2007، 166).

المطلب الثاني

التطور التاريخي لحماية البيانات في القانون الإداري

إن البيانات الشخصية وما يتعلق بها من حماية أقرتها نصوص ضمن قوانين معينة، لم تكن وليدة الصدفة بل إن هذه الحماية أقرت نتيجةً لبعض التطورات السابقة عليها، لذا سنحاول ضمن هذا المطلب بيان التطور التاريخي لحماية البيانات في القانون الإداري، ضمن فرعين وفق ما يلي:

الفرع الأول

نشأة حماية البيانات في القانون العراقي والمصري

في سياق البحث ضمن التشريعات العراقية يتبين أن هناك حماية جزئية للبيانات الشخصية، وذلك من نصوص متفرقة مثل نص المادة (7) من قانون الأحوال المدنية رقم (65) لسنة 1972 التي تؤكد على سرية المعلومات الشخصية في السجلات المدنية، فضلاً عن تجريم إفشاء الأسرار وفقاً للمادتين 437 و438 من قانون العقوبات العراقي رقم 111 لسنة 1969 النافذ، ومع ذلك يظل القانون العراقي بحاجة إلى تشريع شامل وحديث يعالج حماية البيانات الشخصية بصورة تتناسب مع التطورات الرقمية الراهنة.

على حين أن مصر قد اتخذت خطوات كبيرة في هذا الاتجاه فإن الأساس القانوني الذي يحمي البيانات الشخصية الرقمية لكل فرد سواء كان شخصاً طبيعياً أو اعتبارياً، عامّاً كان أو خاصّاً، يتجلى في كونه تجسيداً لمحرّمات الحياة الخاصة وفقاً للدستور المصري (دستور جمهورية مصر العربية، 2019)، ويرتبط ذلك بالحق في الخصوصية كما نصت عليه المواد 54 و92 من الدستور المصري النافذ، وهو أيضاً جزء من حقوق سرية المعلومات المتعلقة بالشخص بحسب ما ورد في المادة (68)، فهذه الحقوق تعد

حقوقاً عامة ودستورية، كما يتضح من المواد 31 و51 و53 و54 و57 و59 و60 و67 و92 و98 و100 في الدستور المصري النافذ، كذلك فإن هذه الحقوق تمثل جزءاً من حقوق الإنسان المعترف بها دولياً إذ تلتزم مصر بتلك الحقوق حال تصديقها على الاتفاقيات والمعاهدات الدولية مما يجعلها ذات قوة قانونية عند نشرها وفق الأطر المقررة في المادة 93 من الدستور المصري النافذ. وتنص المادة (31) من الدستور الحالي الصادر في عام 2014 على أن: "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه وفقاً لما يحدده القانون."، كما تؤكد المادة (51) على أن: "الكرامة حق لكل إنسان، ولا يجوز المساس بها، وتلتزم الدولة باحترامها وحمايتها"، وفي السياق نفسه تشير المادة (53) إلى أن: "المواطنون أمام القانون سواء، وهم متساوون في الحقوق والحريات والواجبات العامة، دون تمييز بينهم لأي سبب من الأسباب." وتعتبر المادة (54) عن أن: "الحرية الشخصية حق طبيعي، مصونة لا تمس، ولا يجوز القبض على أحد أو تفتيشه أو حبسه إلا بأمر قضائي مسبب"، وفيما يتعلق بالحرمة تؤكد المادة (57) على أن: "الحياة الخاصة حرمة تصونها القوانين، وسريتها مكفولة، ولا يجوز الاطلاع عليها أو مصادرتها إلا بأمر قضائي مسبب، ولفترة محددة، وفقاً لما يقره القانون"، لذا يمكن القول بأنه تتكثف التهديدات التي قد تصيب هذه الحقوق نظراً لتنوع الوسائل المستخدمة من التزوير في المحررات الرقمية إلى التحويلات الإلكترونية غير المشروعة.

الفرع الثاني

نشأة حماية البيانات في القوانين الأوروبية

ظهر الحق في حماية الحياة الخاصة ضد أي تدخل لأول مرة في الوثيقة المعروفة باسم "الإعلان العالمي لحقوق الإنسان"، الذي صدر في عام 1948، إذ تنص المادة الثانية عشرة من هذا الإعلان على أنه: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة، أو شؤون أسرته، أو مسكنه، أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص الحق في أن تحميه القوانين من مثل هذا التدخل أو تلك الحملات".

وتأثرت دول أوروبا بشكل كبير بهذا الإعلان الحقوقي إذ اجتمع مجلس أوروبا الذي أنشئ بعد الحرب العالمية الثانية لتعزيز سيادة القانون والديمقراطية وحقوق الإنسان والتنمية الاجتماعية، وأصدر المجلس "الاتفاقية الأوروبية لحقوق الإنسان" عام 1950، التي دخلت حيز التنفيذ في عام 1953 وقد تضمنت الحق في احترام وحماية الحياة الخاصة والأسرية كما هو منصوص عليه في المادة الثامنة.

وفي عام 1959 تم إنشاء المحكمة الأوروبية لحقوق الإنسان لضمان تطبيق مقتضيات الاتفاقية الأوروبية لحقوق الإنسان، إذ أصدرت هذه المحكمة أحكاماً بالاستناد إلى المادة الثامنة في مناسبات عديدة، ومع ظهور تكنولوجيا المعلومات في ستينيات القرن الماضي ظهرت الحاجة الملحة إلى وضع قواعد أكثر تفصيلاً لحماية بيانات الأفراد ذات الطابع الشخصي، لذا أصدرت لجنة وزراء مجلس أوروبا منذ منتصف السبعينيات عدة قرارات تتعلق بحماية هذه البيانات، مستندةً غالباً إلى المادة الثامنة من الاتفاقية (اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا، 1950).

وفي عام 1981 أعلنت اتفاقية أوروبية جديدة تهتم بحماية الأفراد فيما يتعلق بالمعالجة الآلية لبياناتهم ذات الطابع الشخصي، وهي المعروفة بـ "اتفاقية مجلس أوروبا رقم 108" إذ تعد هذه الاتفاقية — حتى وقت قريب — الوثيقة القانونية الوحيدة الملزمة في ميدان حماية البيانات الشخصية، حيث تنطبق على أي معالجة لهذه البيانات سواء في القطاع الخاص أو العام، بما في ذلك المعالجات التي تقوم بها السلطات القضائية أو سلطات إنفاذ القانون، وتسعى هذه الاتفاقية إلى حماية الأفراد من الانتهاكات المحتملة التي قد تترتب على جمع البيانات الشخصية ومعالجتها، كما تنظم تدفق البيانات الشخصية عبر الحدود فتعتمد الاتفاقية 108 على عدة مبادئ جوهرية من أهمها أن يكون جمع البيانات قانونياً ونزيهاً، وأن يهدف لأغراض مشروعة ومحددة، كما تحظر الاتفاقية الاحتفاظ

بالبيانات الشخصية مدة أطول من اللازم، فضلا عن ذلك تمنع الاتفاقية معالجة البيانات الحساسة في غياب الضمانات القانونية الكافية، مثل تلك المتعلقة بالحالة العرقية أو السياسية أو الدينية أو الجنسية للفرد.

إن التوجيه الأوروبي CE/46/95، الذي صدر عن البرلمان والمجلس الأوروبيين بتاريخ 24 أكتوبر 1995 يُعدّ من أبرز التشريعات التي تتناول حماية الأفراد في مواجهة معالجة البيانات الشخصية، فضلا عن تعزيز حرية حركة هذه البيانات، ومنذ ذلك الحين سعت دول أوروبا إلى تضمين هذا التوجيه ضمن قوانينها الوطنية، مما أدى إلى تفاوت في مستوى الحماية القانونية للبيانات الشخصية حسب المنهج الذي اعتمده كل دولة، ويعكس هذا التوجيه رغبة حقيقية في توحيد ومواءمة التشريعات الوطنية الأوروبية ذات الصلة بهذه الحماية حيث يقدّم مستوى من الدقة يتماشى إلى حد كبير مع تلك التشريعات، وهو ما يثبت ما ورد في أحد أحكام محكمة العدل التابعة للاتحاد الأوروبي، حيث جاء فيه: "إن التوجيه CE/46/95 يسعى إلى تحقيق مستوى موحد من حماية حقوق وحرية الأفراد في معالجة البيانات الشخصية عبر جميع الدول الأعضاء.

ومع أن التوجيه الأوروبي لحماية البيانات يقتصر على الدول الأعضاء في الاتحاد الأوروبي أو المنطقة الاقتصادية الأوروبية، فإن الحاجة قد برزت لتأسيس إطار قانوني آخر يهدف إلى إنشاء حماية للبيانات الشخصية ضمن سياق المعالجة من قبل المؤسسات والهيئات الواقعة خارج نطاق الاتحاد الأوروبي، وقد كانت اللائحة رقم 2001/2545 بشأن حماية الأفراد ذات الصلة من ضمن الحلول المطروحة لهذه المهمة (<https://eur-lex.europa.eu/legal>).

علاوة على ذلك، حتى في المجالات التي يغطيها توجيه حماية البيانات الشخصية كانت هناك حاجة مستمرة إلى أحكام أكثر تفصيلاً لتحقيق الوضوح المطلوب، مثل التوجيه رقم 20/58/2002 الذي يتناول معالجة البيانات الشخصية وحماية الحياة الخاصة في قطاع الاتصالات الإلكترونية، فضلاً عن التوجيه رقم 24/2006/المعدل له المتعلق بالاحتفاظ بالبيانات الناتجة عن معالجة خدمات الاتصالات الإلكترونية، وفي هذا السياق يبرز الباحث أهمية توجيه الأنظار نحو وثيقة أساسية أخرى في مجال حماية البيانات الشخصية في أوروبا، وهي ميثاق الحقوق الأساسية للاتحاد الأوروبي (<https://eur-lex.europa.eu/legal>).

المبحث الثاني

المتطلبات الخاصة بحماية البيانات في القانون الإداري وصورها

تتعدد أوجه الحماية الممنوحة للبيانات الشخصية وفقاً للتشريعات المعنية بحمايتها، إذ تُعدّ المعطيات الشخصية جزءاً لا يتجزأ من الهوية الإنسانية تكتسب أهمية كبيرة في تحديد هوية الأفراد، وتُعدّ هذه المعطيات أيضاً أسراراً خاصة إذ يترتب على الإفصاح عنها أو عرضها للغير أو مشاركتها معهم مسؤولية مدنية قد تؤدي إلى تكبد صاحبها خسائر مالية جراء انتشار تلك البيانات مما يستدعي ضرورة التنظيم التشريعي لهذه البيانات، فما هي متطلبات حماية البيانات ضمن القانون العراقي؟، وهل هناك صور خاصة لهذه الحماية؟، وهل هناك معوقات تحول دون تحقيق هذه الحماية؟، هذه التساؤلات سنحاول بيان الإجابة بخصوصها ضمن مطلبين على وفق الآتي:

المطلب الأول

المتطلبات الخاصة بحماية البيانات الشخصية في القانون الإداري

سوف نحاول ضمن هذا المطلب بيان المتطلبات الخاصة بحماية البيانات الشخصية في القانون الإداري، ضمن فرعين:

الفرع الأول

أوجه حماية البيانات الشخصية في القانون العراقي

يعاني النظام القانوني العراقي من نقص واضح في التشريعات الحديثة التي تواكب التغيرات الراهنة في المجتمع، ومنها ضرورة وجود قانون مستقل لحماية البيانات الشخصية ولاسيما تلك التي تستحصلها الإدارات العامة من الأفراد والمؤسسات، وهذا يستدعي التأمل في إمكانية حماية موضوع بحثنا عبر قواعد المسؤولية المدنية المنصوص عليها في القانون المدني.

فقد نصت المادة (240) من القانون المدني العراقي على أنه: "كل تعد يصيب الغير بأي ضرر آخر غير ما ذكر في المواد السابقة يستوجب التعويض" (القانون المدني العراقي، 1951)، ومن هذا النص يتضح أننا أمام مسألة تتعلق بتعويض الأضرار الناجمة عن الأفعال التي تُلحق بالغير الأذى، أن المعطيات التي تدل على شخص ما مثل الاسم، تاريخ الميلاد، الحالة الاجتماعية، والحالة الصحية، إلى جانب فصيلة الدم، المستوى التعليمي وغيرها من المعلومات تصنف تحت بند البيانات الشخصية، لذا يجب فهم طبيعة الفعل الذي يؤدي إلى الإضرار بالشخص نتيجة الاستخدام أو الاطلاع على بياناته الشخصية.

إنّ فعل التعديّ والذي يمكن تسميته بالخطأ التقصيري هو إخلاء بواجب قانوني سابق يستوجب إدراكا وتمييزا، وهذا الالتزام القانوني يهدف إلى احترام حقوق الأفراد وعدم الإضرار بهم، وينطوي على ضرورة بذل العناية المطلوبة لتفادي الأذى الذي قد يلحق بالآخرين (النقيب، بلا تاريخ نشر، 271)، ويُفهم التعديّ على أنه تجاوز للحدود التي ينبغي على الإنسان الالتزام بها في سلوكه، سواء أكان ذلك السلوك متعمداً أو غير متعمد، ومن الضروري أن نفرق بين نوعين من المعايير: معيار التعمد الذي يُقاس موضوعياً لتحديد الانحرافات، وعنصر الإدراك والتمييز الذي يُعد شرطاً أساسياً لتحقيق المسؤولية المدنية (الجمال، 2003، 384). وفي هذا السياق يُعرف الضرر بأنه: "الأذى الذي يُصيب الشخص في حق أو مصلحة مشروعة. وتُعتبر البيانات الشخصية حقاً أو مصلحة مشروعة"، وفقاً للمعنى السابق يُعتبر الضرر أحد الأركان الأساسية التي تقوم عليها المسؤولية ضمن القانون الإداري أسوةً بالقانون المدني، إذ إنّه يلزم التعويض بناءً على مقدار الضرر، وإذا انتفى الضرر انتفت المسؤولية، ولا يمكن المطالبة بالتعويض أو إقامة دعوى بذلك، فإنّ الضرر كعنصرٍ ضروري لقيام المسؤولية التقصيرية للإدارة، يرتبط حتماً بحدوث خطأ من خلال الرابطة السببية بين الخطأ والضرر الناتج عنه. وعلى وجهٍ عام، إذ تقوم المسؤولية التقصيرية للإدارات العامة بموجب إخلال بالواجب القانوني العام الذي يقضي بعدم الإضرار بالغير، حيث يتضمن ذلك الاعتداء على حق مشروع كفله القانون ومنها المعطيات الشخصية، وبالتالي يستتبع أي تعدٍ على تلك البيانات مسؤولية من يتسبب في تلك الأفعال (الجوري، 2011، 65).

إنّ عملية الدخول إلى بيانات شخص ما والاطلاع عليها أو استخدامها دون الموافقة تتطلب تعويضاً حتى وإن لم يكن المتسبب يقصد الضرر فعلياً، شريطة أن لا يكون الفاعل مخولاً لذلك في إطار تأدية واجبه الوظيفي، وفي حال كانت هناك حالة ولوج إلى المعطيات الشخصية بوسيلة غير قانونية ووجد فيها قصد لإحداث الضرر، فإنّ الجواز الشرعي يُخالف الضمان، إذ إنّ من يستخدم حقه استعمالاً مشروعاً لا يتحمل تبعات الأذى الذي ينتج عن ذلك، لذا إذا كان هناك شخص مخول بالوصول إلى البيانات الشخصية لمستخدمي برنامج معين، وترتب على ذلك ضرر، فلا تقوم المسؤولية التقصيرية في هذه الحالة، لأنّ دخول البيانات كان مرصفاً به منذ البداية (الصلصامة، 2002، 192).

وقد منح المشرع المصري المتضرر من الاعتداء على بياناته الشخصية الحق في المطالبة بالتعويض وفق القواعد العامة للمسؤولية المدنية، فضلاً عن العقوبات المنصوص عليها في التشريعات ذات الصلة بالعمل الإداري، وفي حال وجود نصوص تتعلق بعقوبات أشد في قانون العقوبات المصري فإنها تبقى قائمة وتنص المادة (35) من قانون البيانات الشخصية المصري على أنه: "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في أي قانون آخر، ومع عدم الإخلال بحق المضرور بالتعويض"، وقد فرضت عقوبة الغرامة التي تتراوح بين 200 ألف إلى مليونين جنيه مصري على كل من يُجمع البيانات الشخصية بدون وجه حق أو موافقة صاحبها، حيث تُعتبر عملية جمع البيانات جريمة وفقاً لقانون حماية البيانات المصري، بالإضافة إلى ذلك فإن قيام حائز البيانات الشخصية أو المتحكم بها بجمع أو تداول أو معالجة أو إفشاء تلك البيانات دون موافقة صاحبها يوجب عقوبة الغرامة، فضلاً عن عقوبة الحبس التي تمتد لفترة لا تقل عن ثلاثة أشهر، أو غرامة تتراوح بين 500 ألف إلى 5 مليون جنيه، أو عقوبة واحدة منهما على من يخالف حركة البيانات الشخصية عبر الحدود.

لم يُوفق المشرع العراقي في سن قانون البطاقة الوطنية رقم (3) لسنة 2016، إذ اقتصر القانون على كيفية تحويل ونقل القيود المدنية من السجلات الورقية إلى الصيغة الرقمية، وقد منح هذا القانون المواطن بطاقة هوية جديدة بدلاً من هوية الأحوال المدنية

القديمة متضمنةً البيانات الشخصية كافة، وعلى الرغم من ذلك غفل المشرع عن قضايا الاعتداء على تلك البيانات وسبل حمايتها، وأهمل فرض النصوص والعقوبات اللازمة لحمايتها، مما يبرز الحاجة الماسة لإيجاد تشريع كافٍ يضمن حماية البيانات الشخصية للأفراد.

الفرع الثاني

معوقات حماية البيانات الشخصية في القانون الإداري

إن البيانات الشخصية وحمايتها لا تكون عملية متاحة ضمن نطاق التشريعات على حدٍ سواء، إذ إن الحماية المبتغاة لهذه البيانات تستوجب وجود آليات كفيلة بهذا البيانات، لغرض توفير بيئة مناسبة ضمن هذا المضمار، إلا أن هذه الحماية تعترضها معوقات من شأنها إضعاف هذه الحماية أو انعدامها في أحيانٍ أخرى، سنحاول ضمن هذا المطلب بيان ما يخص هذه المعوقات، ضمن مقصدين:

أولاً: ضعف الإدارات الإلكترونية

في عصر التقدم التكنولوجي السريع تبحث معظم الدول عن سبل لتعزيز كفاءة إدارتها من تطبيق مفهوم الحوكمة الإلكترونية والتي تعرف بأنها "استخدام تكنولوجيا المعلومات الرقمية في انجاز المعاملات، وتقديم الخدمات المرفقية، والتواصل مع المواطنين بمزيد من الديمقراطية. ويتم ذلك عن طريق شبكة المعلومات العالمية (الانترنت) وشبكة المعلومات الداخلية (الانترانت) بقصد تحقيق اهداف معينة واهمها تقديم الخدمات الإلكترونية اما بتفاعل بشري او انجاز آلي" (القيسي، 2011، 18)، كما تعرف بأنها: "مقدرة الاجهزة الحكومية المختلفة على توفير الخدمات التقليدية وانجاز المعاملات بسهولة ويسر ودقة متناهية بجهود وتكلفة اقل من خلال موقع واحد على شبكة الانترنت العالمية" (المناعسة — الزعبي، 2013، 27)، إن مفهوم الحوكمة الإلكترونية اشمل من مفهوم الادارة الإلكترونية؛ لان الأخيرة تعني استخدام تكنولوجيا المعلومات في انجاز المعاملات التي تنجز داخل الادارات ابتداءً من المراسلات وانتهاءً بتكامل نظم المعلومات بحيث يصبح كل المهام والنشاطات تنجز باستخدام تكنولوجيا المعلومات، اما الحوكمة الإلكترونية فتعني جعل كافة الادارات الحكومية تتكامل مع بعضها البعض وتقدم الخدمات العامة فيما بينها وبين المواطنين والقطاع الخاص بشكل مباشر. لذلك ان مفهوم الحوكمة الإلكترونية اشمل من الادارة الإلكترونية (الحسن، 2009، 21)، لذا فإن مفهوم الحوكمة الإلكترونية اشمل من مفهوم الادارة الإلكترونية؛ لان الأخيرة تعني استخدام تكنولوجيا المعلومات في انجاز المعاملات التي تنجز داخل الادارات ابتداءً من المراسلات وانتهاءً بتكامل نظم المعلومات بحيث يصبح كل المهام والنشاطات تنجز باستخدام تكنولوجيا المعلومات، اما الحوكمة الإلكترونية فتعني جعل كافة الادارات الحكومية تتكامل بعضها مع بعض وتقدم الخدمات العامة فيما بينها وبين المواطنين والقطاع الخاص بشكل مباشر. لذلك ان مفهوم الحوكمة الإلكترونية اشمل من الادارة الإلكترونية (السالمي، 2009، 33).

وتجدر الإشارة إلى أن نظام الإدارة الإلكترونية هو توجه رقمي جديد سعت من خلاله الحكومة العراقية نحو الحوكمة الإلكترونية، وكانت اولى بواكير التجربة العراقية عام 2004 عندما وقعت وزارة العلوم والتكنولوجيا العراقية عقدا بقيمة 20 مليون دولار مع احدى الشركات البريطانية لتنفيذ مشروع الحكومة الإلكترونية، وكانت خطة الوزارة تتكون من ثلاث مراحل، ضمن المرحلة الاولى والتي مدتها سنتان كان الهدف تأسيس البنية التحتية لتكنولوجيا المعلومات وتقديم الخدمة الى موظفي وزارة العلوم والتكنولوجيا، على حين أن المرحلة الثانية امتدت لمدة خمسة سنوات هدفت الى تقديم الخدمة الى موظفي الوزارات والى القطاع التجاري، بينما نجد أن المرحلة الثالثة اتصفت بكونها بعيدة المدى وتهدف الى تقديم الخدمات الى المواطنين، وقد شاركت وزارة العلوم والتكنولوجيا في مؤتمر جنيف سنة 2003، وفي تونس سنة 2005 فيما يخص البنية التحتية للحكومة الإلكترونية، وبين المجتمعون عن بيئة تمكينية تتضمن الشبكات الفيزيائية التي تربط الوزارات بعضها مع بعض والمواطن والوزارة من خلال شبكات سلكية ولاسلكية من خلالها يتم النفاذ الى الشبكة الدولية للتواصل مع العالم (خلود، 2014، 300).

واستناداً للأمر الوزاري رقم 46 لسنة 2009 تم تأسيس اللجنة الوزارية للحكومة الالكترونية، تتولى مهمة تنسيق برامج الحكومة الالكترونية وتقديم الخدمات الالكترونية ويترأس اللجنة وزير العلوم والتكنولوجيا مع تمثيل واسع من قبل الوزارات العراقية، ونتيجة للتعاون والتنسيق بين اللجنة وبرنامج الامم المتحدة الانمائي سنة 2009 تم اطلاق العديد من المبادرات للحكومة الالكترونية منها :-

1— مؤتمر العراق الالكتروني والحكومة الالكترونية سنة 2009.

2— عقد برنامج في عمان لتدريب المدربين، الاول على الحكومة الالكترونية وورشه عمل التدريب الوطني بالحكومة الالكترونية في اربيل والذي شهد بداية عملية حيوية لبناء قرارات الحكومة الالكترونية في العراق فضلا عن ذلك تنفيذ برنامج تدريب المدربين الثاني.

3— إطلاق بوابة العراق للحكومة الإلكترونية عبر الانترنت والتي تحوي الخدمات العامة المعلوماتية والتفاعلية سنة 2011 (حسين، 2013، ص456)، إن تطبيق نظام الحكومة الإلكترونية له فوائد جمة تتجسد في تطبيق الحكومة الالكترونية التي تمنح للمواطنين فرصة الحصول على السرعة والدقة في تقديم الخدمات على مدار (24) ساعة يوميًا، فضلا عن تقديم الخدمة بشكل جماعي للموضوع الواحد، وهذا بدوره يقلل الازدحام والانتظار في طوابير طويلة، ويجنب الاخطاء البشرية المتعارف عليها في ظل اجراءات الحكومة التقليدية باستخدام الحاسب الالي والذي يزود بالبيانات والمعلومات المتعلقة بجميع الخدمات ومن ثم لا وجود للخطأ في العمل المقدم بحيث يمكن تقديم افضل الخدمات لطالبي الخدمة بأعلى سرعة وجودة ودقة (عبد العال، 2006، 101).

ومن بين فوائد الحكومة الإلكترونية يحد ولو بصورة نسبية من ظاهرة الفساد الاداري وذلك بالمزايا العديدة للحكومة الالكترونية، اذ يتضمن نظام الحكومة الالكترونية اتمام المعاملات بطرق الكترونية ويمكن لصاحب الخدمة الدخول الى الموقع الالكتروني الخاص بجهة الادارة وتحديد الخدمة المطلوبة واجراءاتها ومراحلها والتكلفة المقررة للحصول عليها وبذلك لا توجد اي علاقة مباشرة بين طالب الخدمة والموظف المكلف، وما يترتب على ذلك من فساد اداري، قد يتمثل بطلب مصلحة او رشوة من قبل طالب الخدمة حتى يقوم طالب الخدمة بإنجاز أعماله (القرشي، 2012-36)، وبطبيعة الحال فإن المزايا التي تقدم ذكرها لها أثر ايجابي على نظام حماية البيانات الإلكترونية للمتعاملين مع الإدارة إذ تظهر هذه الأهمية من الكشف عن مصدر تهديد حماية البيانات من جهة، واعتماد نظام الكونوني لحماية هذه البيانات عوضاً عن ضعف الحماية للبيانات المثبتة بطريقة تقليدية للمتعامل مع الإدارة.

ولا شك أن تطبيق المعايير القانونية لحماية الخصوصية وأمن المعلومات على شبكة الإنترنت يعد من صميم اختصاص الحكومة الإلكترونية. ومن هنا تتجلى أهمية إنشاء سلطة إدارية مستقلة، سواء أكانت لجنة لحماية الخصوصية أو نظاماً لفوضى البيانات والخصوصية، تكفل حماية خصوصية مستخدمي الإنترنت، وتسهم في ملاحقة الجرائم الإلكترونية. ولتفعيل دور الحكومة الإلكترونية التي تتولى إيصال الخدمات إلى المواطنين، ينبغي أن تكون البيانات المستخلصة عبر هذه المنظومة خاضعة لنفس الضمانات القانونية المعتمدة في القوانين المقارنة. ويجب أن تحظى بالحماية اللازمة، إذ لا يُسمح بالوصول إليها إلا وفق ضوابط قانونية واضحة ومحددة، وعلى أساس إذن قضائي، وذلك تقديراً لانتهاك حرمة الحياة الخاصة أو تعرض المعلومات للسرقة (الكبيسي، 2008، 40).

لقد أفضى التطور السريع في مجال المعلوماتية إلى الحاجة الملحة لإنشاء هيئة إدارية مستقلة تتولى شؤون حماية خصوصية الأفراد، عبر سن قوانين تتماشى مع مصالحهم وتوفر لهم الحماية اللازمة. فلا ينبغي أن تكون المعلوماتية أداةً للانتقاص من كرامة الإنسان أو المساس بخصوصية حياته. ومن هنا انبثقت فكرة صياغة مشروعات قوانين تتعلق بحماية المعلوماتية في البيئة الرقمية الإدارية، وقد ترجم ذلك إلى واقع ملموس ينظم المعاملات الإلكترونية ويسن الضوابط والأحكام الضرورية. فالمعلومات المسجلة في وحدات المرور والأحوال المدنية تحتوي على بيانات تفصيلية عن الأفراد، بما في ذلك صورهم الشخصية وأسمائهم وأرقام هواتفهم وعناوينهم، فضلاً عن أرقام بطاقاتهم القومية. وهذه البيانات لم تكن محمية بإدارة فعالة (الرفاعي، بلا تاريخ نشر، 311).

غير أن هذا المشروع الجريء في العراق يواجه جملة من العقبات التي تهدد نجاحه واستمراريته من بين أبرز هذه المعوقات تتجلى الصعوبات الإدارية التي تعيق الطريق نحو تحول حقيقي نحو إدارة حديثة تعتمد على تكنولوجيا المعلومات (التميمي، 2007، 166) ، وأمر ضعف الإدارات الإلكترونية يتأتى من عوامل معينة، ومنها:

1. ضعف الرغبة في التغيير

تظهر أولى المعوقات بوضوح في ضعف الرغبة لدى العديد من العاملين في المؤسسات الحكومية لتبني التحولات المطلوبة، ويساهم الجهل بالتكنولوجيا الحديثة بصورة كبيرة في تشكيل تحديات تعوق الانتقال نحو نظام الحوكمة الإلكترونية، فالكثير من الموظفين يواجهون صعوبات جمة في فهم أو التعلم على هذه الأساليب التكنولوجية الحديثة، وتعود هذه الصعوبات إلى غياب الإرادة من قبل الساسة لدفع عجلة التطوير وتحديث الأنماط التقليدية للإدارة، كما تبرز عدم الرغبة في التحول من قبل الموظف الحكومي ذاته الذي قد يسيطر عليه الخوف من المجهول أو الفهم الخاطئ لعالم التكنولوجيا، وعلى الرغم من الأهمية الكبيرة للحوكمة الإلكترونية في تعزيز الشفافية وتحسين الأداء الحكومي فإن هذه العوامل تظل عائقاً رئيسياً أمام تحقيق ذلك (العوادات، 2010، 25).

2. غياب القيادة الجادة والرؤية الشمولية

لقد أصبح من الواضح أن القيادة الفعالة تعد عاملاً أساسياً في نجاح أي مشروع، ولا سيما في الحوكمة الإلكترونية يتطلب الأمر رؤية واضحة وشاملة مدعومة بخطة استراتيجية قوية، إن غياب القيادة الجادة التي تتبنى رؤية مستقبلية يمكن أن يحكم على مشروع الحوكمة بالفشل، إذ تعد عملية التخطيط الإداري هي الأداة الرئيسية لبلورة هذه الرؤية، ويجب أن يتم تصميم خطط تراعي السيناريوهات المحتملة لتكيف مع التغييرات العالمية فالتخطيط المنفصل أو المتسرع يقود إلى نتائج عكسية، إذ ينجم عنه إضعاف المكونات الأساسية اللازمة لنجاح الحوكمة الإلكترونية مما يعرض المشروع للفشل ويؤدي إلى انتهاء العمل به (جراح، 2012، 130).

3. الإعداد غير الكافي للتدريب والتطوير

علاوة على ذلك تبرز مشكلة أخرى تتعلق بالإعداد غير الكافي للتدريب والتطوير، حيث يُستثنى العديد من الموظفين من برامج التدريب المعنية بتطوير المهارات التكنولوجية، وبالتالي فإن برمجيات الحوكمة الإلكترونية تبقى حبراً على ورق ما لم يتم تأهيل الأفراد القائمين على تطبيقها، إن الاستثمار في التدريب المعني بتطوير المستويات المعرفية والمهارية للعاملين هو ضرورة حتمية تساهم في تحقيق النجاح المرجو (التميمي، 2007، 169).

ثانياً: الأمية الإلكترونية وصعوبة التعامل مع التقية الحديثة

تعد التحديات التي تعترض سبيل حماية البيانات في القانون الإداري من أهم القضايا التي تواجه المجتمعات المعاصرة، لا سيما في زمن الحوكمة الإلكترونية والتطور التكنولوجي السريع، وفي هذا السياق تُعد المعوقات البشرية من بين أبرز العقبات التي ينبغي التصدي لها، إذ يُعد العنصر البشري هو العمود الفقري لنجاح أي مشروع بما في ذلك تلك المتعلقة بتطوير الحوكمة الإلكترونية، فبدون الكوادر المؤهلة لا يمكن تحقيق الأهداف المنشودة، إن قلة العدد وعدم تأهيل الكوادر البشرية في العراق تُمثل تحدياً حقيقياً تجاه التكيف مع متغيرات التكنولوجيا الحديثة، وذلك أن غياب الخبرات اللازمة للانتقال من الأنماط التقليدية إلى الأساليب الإلكترونية يشكل عقبة كبيرة يجب التخلص منها ومن بين التحديات الأساسية التي تواجه هذا التحول تبرز الأمية المعلوماتية كأهم هذه العقبات (يحيى، 2015، 15).

تُعد الأمية المعلوماتية من الأفات التي يعاني منها العراق إذ يُواجه الأفراد صعوبة كبيرة في التعامل مع الحواسيب وتقنيات المعلومات الحديثة، هذا وإن التخلص من هذه الأمية يتطلب جهوداً جبارة من قبل المؤسسات الأكاديمية، ومعاهد التعليم، فضلا عن الدوائر الحكومية والقطاع الخاص، إذ يتعين على الجامعات والمدارس تقديم برامج تثقيفية شاملة تبرز أهمية استخدام الحاسوب كأداة

لا غنى عنها في بناء الأمم وتقدمها، ومن الضروري أن تتضمن هذه البرامج تدريباً فعالاً يُحرر الأفراد من المخاوف المرتبطة بالتكنولوجيا، والعمل على تسهيل استخدام الحواسيب، وأيضاً تعزيز قدرات المدربين وتزويدهم بالأدوات والأساليب اللازمة ليصبحوا أكثر كفاءة ومرونة في تقديم التعليم في مجال التقنيات الحديثة (يحيى، 2015، 17).

ومن جهة أخرى، يُعد العائق اللغوي وجهاً آخر للأمية وهي من أبرز التحديات التي تعترض عملية استخدام الإنترنت في العراق. إذ تفتقر المؤسسات الحكومية إلى الكوادر القادرة على التواصل بلغة العصر الحديث، ألا وهي اللغة الإنجليزية. إذ إن اللغة الإنجليزية تمثل اللغة الأساسية للإنترنت، إذ يُقدر أن أكثر من 80% من المحتويات الإلكترونية متوفرة بهذه اللغة. ومن ثم، يُصبح من الضروري أن يتمكن الموظفون من تطوير مهاراتهم اللغوية، ليس فقط لفهم المعلومات، بل أيضاً للمشاركة الفعالة في الفضاء الرقمي الذي يضم العديد من الفرص. إن الحلول التي يمكن أن تُطرح لمواجهة هذه المعوقات متعددة، وتتطلب تعاوناً وثيقاً بين مختلف المؤسسات. إن الحد من الأمية المعلوماتية وتعليم اللغة الإنجليزية يشكّلان عاملاً جوهرياً لإجراء تحول حقيقي نحو الحوكمة الإلكترونية. لذا، ينبغي إعداد برامج تعليمية متكاملة تأخذ في الاعتبار احتياجات المجتمع وتوجهاته (المعري، 2010، 15).

المطلب الثاني

مسؤولية الإدارة عن الإخلال بحفظ البيانات الشخصية وصورها

إن الإدارات العامة بوصفها أشخاصاً عامة تهدف لتحقيق النفع العام وتحقيق المصلحة العامة لا يعد مبرراً لإعفائها من المسؤولية التي تتحقق من جراء عم المحافظة على البيانات الشخصية للأفراد المتعاملون مع الإدارة، ويكمن أساس مسؤولية الإدارة عن حماية البيانات تكمن في علاقة التبعية بين الموظف والإدارة، إذ إن القانون العراقي أرسى هذه العلاقة ضمن القانون المدني والتي يمكن اعتماده ضمن القانون الإداري حيث نصت المادة (219) ضمن فقرتها الأولى من القانون المدني العراقي تنص على: "الحكومة والبلديات والمؤسسات الأخرى التي تقوم بخدمة عامة وكل شخص يستغل احد المؤسسات الصناعية او التجارية مسؤولون عن الضرر الذي يحدثه مستخدموهم، اذا كان الضرر ناشئاً عن تعدد وقع منهم اثناء قيامهم بخدماتهم"، فالمادة (219) من القانون المدني العراقي رقم (40) لسنة 1951 والمتعلق بمسؤولية المتبوع عن أعمال تابعه، تؤكد أن التبعية موضوع البحث هي علاقة تقوم بين شخصين أو أكثر، يكون لاحدهم وهو المتبوع سلطة فعلية في الرقابة والتوجيه على الآخر وهو التابع وذلك بخصوص عمل معين يقوم به الأخير لمصلحة المتبوع وحسابه، سنحاول ضمن هذا المطلب بيان مسؤولية الإدارة عن الإخلال بحفظ البيانات الشخصية وصورها، ضمن فرعين:

الفرع الأول

موقف القانون العراقي من مدة الاحتفاظ بالبيانات الشخصية

إن إبرام أي عقد سواءً ضمن القانون الخاص أو القانون العام يتطلب تحقيق آثار تتجلى في الحقوق والالتزامات المتبادلة بين الأطراف ولكن تختلف طبيعة هذه الآثار ومداهها وفقاً للقانون الذي ينظمها فالعقود الإدارية التي تبرمها الإدارات العامة تكون سبباً في حصول بعض الموظفين على البيانات والأسرار الخاصة بالمتعاملين مع الإدارة، وعلى الرغم من عدم وجود نص صريح يلزم الموظف بالمحافظة على الأسرار، أو عدم وجود اتفاق في العقد يخص هذا الالتزام، يتبادر السؤال: هل يعني ذلك أن الموظف غير ملزم بالسرية؟ في هذه الحالة، يُعد التزام الموظف من حيث المبدأ قائماً على وفق مبدأ حسن النية في تنفيذ العقود، إذ نصت المادة 150 من القانون المدني على ضرورة تنفيذ العقد حسب ما تضمنه وبطريقة تتماشى مع متطلبات حسن النية. فحسن النية يتطلب حتماً المحافظة على أسرار العمل كونها تمس مصلحة صاحبها، وأي إفشاء لتلك الأسرار يُلحق الضرر بتلك المصلحة. كما تبين الفقرة الثانية من نفس المادة أن الالتزام بالسرية يُعتبر من مستلزمات العقد، إذ يندرج تحت نطاق التزاماته وفقاً للقانون والعرف والعدالة (القانون المدني العراقي، 1951).

إن خطر إفشاء بيانات المتعاملين مع الإدارة لا يقتصر على مدة تنفيذ العقد فحسب، بل يستمر حتى بعد انقضائه، فإذا اقتصر تحريم إفشاء تلك الأسرار على مدة تنفيذ العقد، فإن الموظف أو أي شخص له علاقة مع الإدارة يمكنه أن يتحايل على هذا التحريم بإنهاء العقد بسرعة أو فسخه، ليستفيد من الأسرار التي اطلع عليها بموجب عمله، لذلك، حرصت التشريعات على الاستمرار في حماية السرية وحفظ البيانات الشخصية (يحيى، 1989، 187).

أما في حال عدم وجود اتفاق صريح في العقد يخص الالتزام بالسرية بعد انتهاء مدة العقد، فإن الحفاظ على أسرار العمل يعد من الضرورات التي تتطلب التنفيذ بحسن نية، وفقاً لما ورد في الفقرة الثانية من المادة 150 من القانون المدني العراقي رقم 40 لسنة 1951، ومن ثم فإن إفشاء العامل لأسرار العمل بعد انتهاء العقد يمكن أن يسبب ضرراً لرب العمل، مما يتعارض مع مبدأ حسن النية.

هكذا يصبح الالتزام بالحفاظ على أسرار العمل بعد انتهاء العقد التزاماً قانونياً عاماً، يفرضه القانون ويعد أمراً مفترضاً طالما أن المعلومات تنتم بالسرية، لذلك فهذا الالتزام لا يقتصر على فترة تنفيذ العقد فقط، بل يمتد ليشمل ما بعد انقضاء العقد، وهي مرحلة من أخطر المراحل في حال عدم وجود اتفاق واضح حول ذلك، لذا فإن التزام الحفاظ على السرية بعد انتهاء العقد يستند إلى أحكام القانون التي تقتضي عدم الإضرار بالغير، وقد رتب ذلك المسؤولية التقصيرية المتمثلة بالتعويض مما يؤدي إلى توفير الحماية الكافية لأسرار العمل (ابو شنب، 2006، 156).

وتكمن أهمية الالتزام بالحفاظ على أسرار العمل في كونه يمتد ليشمل المدة التي تتجاوز انتهاء العقد بين المتعاقد والإدارة، في هذا السياق يتبنى المشرع في العديد من الدول العربية، مثل مصر والأردن نظرة تقتضي بأن يظل هذا الالتزام سارياً حتى بعد انتهاء العقد، لكن يُظهر القانون العراقي بموجب قانون العمل رقم 37 لسنة 2015 تبايناً واضحاً حيث قصر مدة الالتزام بالسرية على مدة سريان العقد فقط، مما يتعارض مع النصوص السابقة في قانون العمل الملغى رقم 71 لسنة 1987 الذي دعا إلى استمرار هذا الالتزام بعد انقضاء العقد، حظراً على العامل إفشاء الأسرار التي اطلعت عليها في مدة عمله.

الفرع الثاني

موقف القانون المصري والأوروبي من مدة الاحتفاظ بالبيانات

إن الإدارة في جوهرها تجسيد لتفاعل بشري محوري ينطلق من جهود الأفراد الذين يعملون تحت مظلتها، ويسعون جاهدين لتحقيق المصلحة العامة، فهؤلاء الأفراد الذين يوصفون بـ"الموظفين العموميين"، يجسدون قيمة لا تقتصر على أدائهم لوظائفهم، بل تتجاوز ذلك إلى إسهامهم في بناء المؤسسة الإدارية وتعزيز كفاءتها، وهذا البناء لا يغفل شرعية وجوده إذ تحكمه القوانين والأنظمة الخاصة بالوظيفة العامة الهادفة إلى تنظيم أدوار هؤلاء الأفراد وتأمين حسن أدائهم فندرك القوانين المتعلقة بالخدمة المدنية أهمية الموظف كحلقة وصل بين الإدارة والجمهور، لذلك فإن النجاح في تحقيق الأهداف المرجوة يتوقف وبشكلٍ جوهري على مدى كفاءة وإخلاص هؤلاء الموظفين وإن احساسهم بالمسؤولية ورغبتهم الصادقة في خدمة المجتمع يُعتبران عاملين حاسمين في أي إدارة ترغب في تحقيق مكانة مرموقة في خدمة الجمهور (الجبوري، بلا تاريخ نشر، 120).

فواجب الموظف في كتمان الأسرار الوظيفية يمثل أحد الأسس الجوهرية التي توطر العمل الإداري، وهذا الواجب يتجذر في العديد من النصوص القانونية التي تسنها التشريعات الوظيفية في فرنسا، ينص القانون الوظيفي رقم 84-6 أ الصادر في 11 يناير 1984، في مادته السادسة والعشرين، على التزام الموظف بالحفاظ على الأسرار الوظيفية التي تصل إلى علمه. كما تشدد المادة السادسة والعشرون من القانون رقم 83-63 الصادر سنة 1983 على أهمية احترام الأسرار المهنية مشيرة إلى القواعد المنصوص عليها في القانون الجنائي التي تضمن حماية هذه الأسرار، علاوة على ذلك تعنتي المادة 226 من قانون 1992 بتجريم إفشاء المعلومات السرية التي يطلع عليها الشخص بحكم عمله أو بصفته المهنية (العربي، بلا تاريخ نشر، 579)، وقد تجلّى حرص المشرع الفرنسي في إقرار التزام الموظف بكتمان الأسرار، إذ أوجب عليه الحفاظ على سرية جميع الوقائع والمستندات والمعلومات

المتعلقة بالإدارة في اثناء ممارسته لوظيفته بصرف النظر عن الوسيلة التي يتم بها الإفصاح سواء كان ذلك من طريق الحديث الشفوي، أو الكتابات الرسمية، أو حتى التصريحات الصحفية (العربي، بلا تاريخ نشر، 580).

وفي سياق متصل أغلق مجلس الدولة الفرنسي الباب أمام التحايل على هذا الالتزام، إذ أكد أنه لا يعدل من طبيعة السرية والقرارات المرتبطة بها أن يتم الإفشاء بناءً على طلب أحد الأفراد لتحقيق مصلحة مشروعة، وتجلي ذلك في قضية Batton، الذي عمل سكرتيراً بأحد أقسام الشرطة ثم أحيل إلى المعاش تأديبياً فتقدم بطلب للتسجيل في نقابة المحامين، وطلب استعلاء الوزارة عن أسباب إحالته، إلا أن الوزارة رفضت الطلب. وبعد ذلك، دعا Batton أمام مجلس الدولة ضد وزارة الداخلية، لكن المحكمة رفضت دعواه لعدم وجود نص قانوني يلزم الإدارة بالكشف عن أسباب الجزاءات التأديبية التي تتخذها بحق أعضائها (خليل، 2002، 443)، أما في مصر فقد تم التأكيد على هذا الواجب أيضاً في تشريعات التوظيف، فقد نص قانون رقم 210 لسنة 1951 على أن مستخدمى الحكومة لا يجوز لهم إفشاء معلومات تتعلق بمسائل سرية، كما تنص القوانين اللاحقة مثل قانون العاملين بالدولة رقم 47 لسنة 1978، على أن الموظف العام محظور عليه إفشاء الأسرار التي يطلع عليها بسبب وظيفته، ويستمر هذا الالتزام حتى بعد تركه الخدمة.

لذا فإن واجب كتمان الأسرار الوظيفية في القانون المصري يتجلى بوضوح من حظر نشر أي معلومات تتعلق بالعمل عبر الصحف أو وسائل الإعلام، فقد صدر عن مجلس الدولة فتوى تنص على عدم جواز إعطاء الأخبار للصحف أو نشر أي ملاحظات شخصية. كما يتوجب على الموظف حفظ الوثائق الرسمية وعدم العبث بها أو تسريبها، لأن ذلك قد يؤدي إلى تفشي معلومات حساسة قد تضر بالمصالح الوطنية (خليل، 2002، 451)، إجمالاً يظهر أن التزام الموظف بكتمان الأسرار الوظيفية لا يقتصر على مصلحة العمل فحسب، بل يمثل صمام أمان لحماية المعلومات الحيوية التي قد تستغلها أطراف خارجية لأغراض قد تكون ضارة بالأمن أو الاستقرار، ومن مراجعة موقف القضاء العراقي والمصري لم نعثر على حكم خاص بحماية البيانات الخاصة بالمتعامل مع الإدارة. في خاتمة بحثنا لما تقدم لموضوع حماية البيانات الخاصة بالمتعامل مع الإدارة نجد بالضرورة إضافة مادة قانونية إلى قانون الخدمة المدنية تقضي بما يلي: "يعاقب الموظف الذي يكون على اطلاع على بيانات شخصية إلكترونية بسبب منصبه الوظيفي تخص متعامل مع الإدارة سواء كان شخص طبيعى أو معنوي بالحبس والغرامة متى ما تم تسريب للجمهور هذا المعلومات عن طريق وسيلة إلكترونية أو أي وسيلة أخرى، ويكون للمتضرر من فعل الموظف حق المطالبة بالتعويض المدني متى ما أضرت هذه المعلومات شخصه أو مركزه الاجتماعي أو سمعته المالية"، وكوسيلة لحماية البيانات الإلكترونية نجد من الأفضل ربط الأجهزة الإلكترونية والحواسيب بنظام مراقبة إلكتروني يكون قادر على كشف تناقل المعلومات الإلكترونية أو نشرها أو نقلها لجهاز أو حاسوب آخر، ولتأكيد الحماية نجد من الضروري نقترح على المشرع العراقي الإسراع في تشريع قانون خاص ومتكامل لمكافحة الجرائم المعلوماتية، يواكب التطور المتسارع في تقنيات الذكاء الاصطناعي وتطبيقاتها الحديثة على أن يتضمن هذا القانون إطاراً قانونياً دقيقاً ينظم استخدام هذه التقنيات ويُجرم بصورة صريحة كل فعل أو سلوك ينطوي على إساءة توظيفها، ونؤكد بوجه خاص على ضرورة إدراج نصوص قانونية واضحة تجرم جريمة الاحتيال باستخدام تقنيات الذكاء الاصطناعي التي تعتمد على استغلال الخوارزميات والأنظمة الذكية في الخداع أو التضليل أو انتحال الهوية أو التلاعب بالبيانات والمعلومات بقصد الاستيلاء على الأموال أو تحقيق منافع غير مشروعة، كما نقترح أن تُقرر لهذه الجريمة عقوبات مشددة ورادعة تتناسب مع خطورتها وطبيعتها التقنية الخاصة.

ونقترح تعديل نص المادة (٧) من مشروع قانون مكافحة الجرائم المعلوماتية لتشمل صراحة استخدام تقنيات الذكاء الاصطناعي والخوارزميات، بحيث يصبح النص كالآتي: "يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠,٠٠٠,٠٠٠) عشرة ملايين دينار ولا تزيد على (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دينار كل من:-

أولاً: استخدم عمداً نظام الحاسوب أو شبكة المعلومات، أو أي تقنيات ذكاء اصطناعي أو خوارزميات ذكية تابعة للأشخاص أو الشركات أو الهيئات أو المصارف أو الأسواق المالية، وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الإلكترونية.

ثانياً: توصل من طريق أجهزة الحاسوب أو شبكة المعلومات أو تقنيات الذكاء الاصطناعي إلى الاستيلاء لنفسه أو لغيره على برامج أو معلومات أو بيانات أو شفرات في أي معاملة أو تعاقد إلكتروني أو بطاقات إلكترونية أو مال منقول أو سند أو توقيع على سند، باستخدام طرق احتيالية أو اتخاذ اسم كاذب أو صفة غير صحيحة من شأنها خداع المجنى عليه"، كما تقترح على المشرع العراقي تعديل نظام التصديق الإلكتروني الذي حدده ضمن قانون التوقيع الإلكتروني عن طريق اشتراط الحصول على المؤهل الفني بخصوص طلب شهادة التصديق الإلكتروني ولا سيما لمبرمجي وشركات الذكاء الاصطناعي، لذا فإن المادة (8) من قانون التوقيع الإلكتروني يجب تعديلها.

الخاتمة:

أولاً: النتائج

1. في السياق القانوني العراقي لم نجد أطرا خاصة للمسؤولية التقصيرية تحت نطاق القانون الإداري وهذا ينعكس سلبيًا على أهمية حماية الأفراد من الأضرار التي قد تنجم عن أفعال غير مشروعة ناشئة عن تعدي يصيب البيانات الشخصية للأفراد، فوجود هذا التوجه التشريعي يعكس التطور في معالجة قضايا التعويض في القضاء العراقي.
2. لم نجد ضمن القانون الإداري تحديد للعقوبة المترتبة على جريمة إفشاء الأسرار الوظيفية، ويتضح أن القانون العراقي قد أتاح للمحكمة السلطة التقديرية في اختيار العقوبة المناسبة، مما يعني أن القاضي يمكنه استنباط العقوبة المناسبة من تفاصيل القضية المطروحة أمامه. وقد وضعت القوانين العراقية سقفًا للعقوبة بالسجن لا يتجاوز السنتين، بينما تركت تحديد الحد الأدنى للغرامة وتفاصيلها لتقدير المحكمة.
3. إن البيانات الشخصية تتمثل في أي معلومات تعكس شخصية الفرد، مثل صورته أو بصماته، وتستند إلى صفاته الجسدية أو السلوكية أو الاجتماعية أو الاقتصادية، مما يتيح التعرف على هويته. وتتضمن هذه المعلومات أيضًا أي بيانات تتعلق بالشخص بطرق غير مباشرة، وبالتالي، تُعد تلك المعلومات معيارًا يحدد ما إذا كانت تحمل الطابع الشخصي، وعند تحقق هذا الشرط، تُصنف على أنها بيانات شخصية تستحق الحماية القانونية.
4. إن التوجيه الأوروبي CE/46/95، الذي صدر عن البرلمان والمجلس الأوروبيين بتاريخ 24 أكتوبر 1995م، يُعد من أبرز التشريعات التي تتناول حماية الأفراد في مواجهة معالجة البيانات الشخصية، فضلًا عن تعزيز حرية حركة هذه البيانات، منذ ذلك الحين، سعت دول أوروبا إلى تضمين هذا التوجيه ضمن قوانينها الوطنية، مما أدى إلى تفاوت في مستوى الحماية القانونية للبيانات الشخصية، حسب المنهج الذي اعتمده كل دولة. ويعكس هذا التوجيه رغبة حقيقية في توحيد ومواءمة التشريعات الوطنية الأوروبية ذات الصلة بهذه الحماية، حيث يقم مستوى من الدقة يتماشى إلى حد كبير مع تلك التشريعات.
5. تعد التحديات التي تعترض سبيل حماية البيانات في القانون الإداري من أهم القضايا التي تواجه المجتمعات المعاصرة، لا سيما في زمن الحوكمة الإلكترونية والتطور التكنولوجي السريع. وفي هذا السياق، تُعد المعوقات البشرية من بين أبرز العقبات التي ينبغي التصدي لها. إذ يُعتبر العنصر البشري هو العمود الفقري لنجاح أي مشروع، بما في ذلك تلك المتعلقة بتطوير الحوكمة الإلكترونية. فبدون الكوادر المؤهلة، لا يمكن تحقيق الأهداف المنشودة. إن قلة العدد، وعدم تأهيل الكوادر البشرية في العراق، تُمثل تحديًا حقيقيًا تجاه التكيف مع متغيرات التكنولوجيا الحديثة. ذلك أن غياب الخبرات اللازمة للانتقال من الأنماط التقليدية إلى الأساليب الإلكترونية يشكل عقبة كبيرة يجب التخلص منها. ومن بين التحديات الأساسية التي تواجه هذا التحول، تبرز الأمية المعلوماتية كأهم هذه العقبات.

6. لم تتطرق التشريعات الحالية لتعريف المسؤولية الانضباطية بشكل شامل، ولكن الفقه قد قدم عدة تفسيرات حول الجريمة الانضباطية، حيث عُرفت في الفقه الفرنسي بأنها أي فعل أو امتناع مخالف للواجبات المفروضة على الموظف فإذا تم النظر إلى المسؤولية الانضباطية على أنها مرتبطة بالفعل المخالف للأداء الوظيفي، فإن تعريف الجريمة الانضباطية يعكس جوهر هذه المسؤولية. وقد عُرِّفت الجريمة الانضباطية بمدى إخلال الموظف بمسؤولياته، مما يستدعي التدخل الانضباطي، تتكون المسؤولية الانضباطية من تصرفات الموظف التي تتسم بالخطيئة أو الذنب في سياق وظيفته. فإذا اكتسب الفرد الوضعية الوظيفية وأخطأ في أداء واجباته، فإنه سيخضع لنظام المساءلة التأديبية، والتي تهدف إلى تصحيح سلوكه وتحفيزه على الالتزام بالمعايير المطلوبة مستقبلاً، خاصة فيما يتعلق بحماية الأسرار الوظيفية لضمان سير العمل بشكل منتظم.

7. في ظل العلاقات الإنسانية المعقدة التي تربط الأفراد بالسلطات، تتبدى خصائص المسؤولية بشكل واضح. فالمسؤولية المدنية تترتب على أي تعدي على حقوق الآخرين، سواء كان ذلك من قبل دائرة حكومية أو مؤسسة أو أفراد يتعاملون مع الموظف المعني، مما يجعل من الصعب تحديد الأخطاء التي تستدعي تلك المسؤولية بشكل عام. أما المسؤولية الجزائية، فتتعلق بسلوك يمس المجتمع بأسره، حيث تُطبق قاعدة: «لا جريمة ولا عقوبة إلا بنص». ومن هذا المنطلق، نجد أن نطاق المسؤولية الجزائية المترتبة على إفشاء الأسرار الوظيفية تتسع مقارنةً بالمجال المدني، إذ تنشأ الأولى من خرق للالتزام القانوني، بخلاف الثانية التي تخضع لقواعد محددة.

8. يحظر على الموظف أو المكلف بالخدمة العامة، الاحتفاظ بأصل الوثائق الرسمية السرية المتعلقة بمهامه الوظيفية. يرتبط هذا الأمر ارتباطاً وثيقاً بحظر إفشاء الأسرار الوظيفية، إذ نصت المادة الرابعة البند 7 من قانون انضباط موظفي الدولة والقطاع العام في العراق، على عدم جواز احتفاظ الموظف بوثائق سرية، وذلك القيد يستمر حتى بعد انتهاء خدماته بصرف النظر عن الطريقة. كما أن الالتزام بالحفاظ على الأسرار وكتمانها ينطبق على المعلومات المتعلقة بالأعمال التي يجريها الموظف، والتي تخص الأفراد الذين يقصدون دوائر الدولة للحصول على خدماتهم أو لقضاياهم الخاصة. ويشمل هذا الواجب أيضاً الأسرار المتعلقة بالهيئة التي يعمل بها الشخص، حتى وإن اطلع عليها بأي وسيلة كانت.

ب-التوصيات

- 1- أهم نص القانون الذي يدل على حماية البيانات الشخصية في الدستور العراقي هي المادة 17 الذي ينص على: «لكل فرد الحق في الخصوصية الشخصية بما لا يتنافى مع حقوق الآخرين والأداب العامة» لكن هذا لا يعد كافياً لأنها لا تنص صراحةً على حمايتها فنوصي بتطوير تشريعات وطنية واضحة وحاسمة تتعلق بحماية البيانات الشخصية في إطار النظام الحكومي الإلكتروني، تشمل معايير محددة لجمع البيانات، ومعالجتها، وتخزينها.
- 2- كما نوصي بأن يتم توفير برامج تدريبية مستمرة للعاملين في الأجهزة الحكومية بشأن قوانين حماية البيانات الشخصية وكيفية الالتزام بها، مما يعزز من ثقافة الخصوصية والأمان داخل المؤسسات.
- 3- نوصي العمل على تكامل الأنظمة الحكومية الإلكترونية مع قواعد بيانات حماية البيانات الشخصية لضمان الاحترام التام للخصوصية عند تبادل المعلومات بين الجهات الحكومية..
- 4- نقترح على المشرع إيراد نص ضمن القوانين العقابية خاص بجرائم الاعتداء على المستندات الإلكترونية لضمان حماية هذه المستندات من جهة، وتوفير الأمان القانوني الذي يخص المستندات الإلكترونية.
- 5- نقترح على المشرع العراقي تعديل نظام التصديق الإلكتروني الذي حدده ضمن قانون التوقيع الإلكتروني عن طريق اشتراط الحصول على المؤهل الفني بخصوص طلب شهادة التصديق الإلكتروني ولاسيما لمبرمجي وشركات الذكاء الاصطناعي، لذا فإنّ المادة (8) من قانون التوقيع الإلكتروني يجب تعديلها وفق ما تقدم.

6— نقترح تعديل نص المادة (٧) من مشروع قانون مكافحة الجرائم المعلوماتية لتشمل صراحة استخدام تقنيات الذكاء الاصطناعي والخوارزميات، بحيث يصبح النص كالآتي: "يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠,٠٠٠,٠٠٠) عشرة ملايين دينار ولا تزيد على (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دينار كل من: - أولاً: استخدم عمداً نظام الحاسوب أو شبكة المعلومات، أو أي تقنيات ذكاء اصطناعي أو خوارزميات ذكية تابعة للأشخاص أو الشركات أو الهيئات أو المصارف أو الأسواق المالية، وتمكن من الاستيلاء على أموال الغير أو حقوقهم المالية أو حقق لنفسه أو لغيره منفعة مالية أو حرم الغير من حقوقه المالية بأية وسيلة من الوسائل الإلكترونية. ثانياً: توصل عن طريق أجهزة الحاسوب أو شبكة المعلومات أو تقنيات الذكاء الاصطناعي إلى الاستيلاء لنفسه أو لغيره على برامج أو معلومات أو بيانات أو شفرات في أي معاملة أو تعاقد إلكتروني أو بطاقات إلكترونية أو مال منقول أو سند أو توقيع على سند، باستخدام طرق احتيالية أو اتخاذ اسم كاذب أو صفة غير صحيحة من شأنها خداع المجنى عليه".

قائمة المصادر

أولاً: الكتب

1. أحمد عبدالكريم ابو شنب، شرح أحكام قانون العمل وفقاً لأحدث تعديلات، ط2، دار الثقافة للنشر والتوزيع، عمان، 2006.
2. أمال قارة، الحماية الجزائرية للمعلوماتية في التشريع الجزائري، ط2، دار هومة للطباعة والنشر، الجزائر، 2007.
3. اسامة المناعسة، احمد الزعبي، الحكومة الالكترونية بين النظرية والتطبيق، ط1، دار الثقافة للنشر والتوزيع، عمان، 2013.
4. سليم الجبوري، الحماية القانونية لمعلومات شبكة الانترنت، بيروت، منشورات الحلبي الحقوقية، بيروت، 2011.
5. خلود عبد الخالق السالم، الحكومة الالكترونية تكنولوجيا المعلومات ودورها في تحقيق الحكومة الالكترونية وانعكاسها على المدينة، ط1، دار الكتب العلمية، بغداد، 2014.
6. علاء عبد الرزاق السالمي، الادارة الالكترونية، ط2، دار وائل للنشر، عمان، 2009.
7. عاطف النقيب، النظرية العامة للمسؤولية الناشئة عن الفعل الشخصي (الخطأ والضرر)، منشورات عويدات، لبنان، بلا تاريخ نشر.
8. عبد الحميد محمد العربي، ممارسة الموظف للحريات العامة في القانون الإداري والقانون الدولي، بلا تاريخ نشر.
9. عبدالعزيز اللصاصمة، المسؤولية التقصيرية للفعل الضار، دار العلمية للنشر، عمان، 2002.
10. عبدالودود يحيى، شرح قانون العمل، ط3، دار النهضة العربية، القاهرة، 1989.
11. علي عبدالفتاح محمد خليل، الموظف العام وممارسة الحرية السياسية، ط1، دار النهضة العربية، القاهرة، 2002.
12. ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الاسكندرية، 1999.
13. ماهر صالح الجبوري، مبادئ القانون الإداري، بغداد، المكتبة القانونية، بلا تاريخ نشر.
14. محمد كمال شرف الدين، قانون مدني النظرية العامة الأشخاص اثبات الحقوق، مطبعة الرسمية، تونس، 2002.
15. مصطفى الجمال، مصادر واحكام الالتزام، منشورات الحلبي الحقوقية، بيروت، 2003.
16. هدى محمد عبد العال، التطور الاداري والحكومة الالكترونية، دون دار نشر، القاهرة، 2006.

ثانياً: الأطاريح والرسائل الجامعية

1. بن عاشور، صليحة بن عاشور، توريث الحقوق والايضاء بها، أطروحة دكتوراه، جامعة الجزائر، 2007.
2. عبدالسلام العومان، الحماية الجزائية للبيانات الشخصية في التشريع الأردني، رسال ماجستير، جامعة الشرق الأوسط، 2022.
3. عمر القريشي، اثر الحكومة الالكترونية في الحد من ظاهرة الفساد الاداري، رساله ماجستير، جامعة النهريين، كلية الحقوق، 2012.
4. كلثم محمد الكبيسي، متطلبات تطبيق الإدارة الإلكترونية في مركز نظم المعلومات التابع للحكومة الإلكترونية في دولة قطر، رسالة ماجستير، كلية ادارة الاعمال، قطر، 2008.
5. يوسف بو جمعة، حماية الحقوق الشخصية، رسالة ماجستير جامعة الجزائر، 2012.

ثالثاً: البحوث

1. أحمد العوادات، المعوقات والصعوبات التي تخول جون تطبيق برنامج الحكومة الالكترونية، عمان، جامعة اربد، مجلة العلوم الاقتصادية والادارية، الأردن، 2010.
2. أحمد قاسم السوداني، واجب الموظف في كتمان السر الوظيفي دراسة مقارنة، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد 10 ، العدد 38، 2021.
3. أنور يحيى، الحكومة الالكترونية بين التحديات والمخاطر، بيروت، مجلة الالكترونية بين التحديات والمخاطر، ع 20، 2015.
4. حسام الدين الاهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الالى، القاهرة، جامعة عين شمس، مجلة العلوم القانونية و الاقتصادية، ع 2، 1990.
5. حنان القيسي، الادارة الالكترونية وتقديم الخدمات العامة، بحث منشور، مجلة الحقوق ، المجلد 4 ، العددان 16، 17 ، 2011.
6. حسين بن محمد الحسن، الادارة الالكترونية بين النظرية والتطبيق بحث مقدم الى معهد الادارة العامة ، المؤتمر الدولي للتنمية الادارية نحو اداء متميز في القطاع الحكومي ، 2009، ص 21. منشور على الموقع الالكتروني www.fifty.ipa.edu.sa ، تاريخ الزيارة 2026/5/14.
7. رزق علي، الحماية الجنائية للبيانات الشخصية المعالجة الكترونيا في ضوء القانون رقم 151 لسنة 2020م، جامعة السادات، ورقة بحثية لمؤتمر العلمي الأول لكلية الحقوق في الجامعة، 2022.
8. سامح التهامي، ضوابط معالجة البيانات الشخصية، بحث منشور في وقائع المؤتمر الدولي، كلية القانون الكويتية العالمية، 2014.
9. سحر قدوري الرفاعي، الحكومة الإلكترونية وسبل تطبيقها مدخل استراتيجي، مجلة شمال افريقيا، ع 7، الجزائر، بلا تاريخ نشر.
10. ليلى علي جمعة، اعتماد الجمهور على مواقع التواصل الاجتماعي في اوقات الأزمات أزمة ارتفاع سعر صرف الدولار أنموذجا، بحث منشور في مجلة لارك، العدد 5، المجلد 14، جامعة واسط — كلية الآداب، 2022، <https://doi.org/10.31185/lark.Vol4.Iss47.2436>
11. طارق جمعة راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، ع 72، القاهرة، 2019.
12. علاء حسين التميمي، ادارة المرفق العامة في ظل الحكومة الالكترونية، مجلة المعهد العربي الثقافي، ج 3، ع 3، عمان، 2007.
13. فهد محمود المعمرى، الحكومة الالكترونية، مسقط، مؤتمر مسقط، سلطنة عمان، 2010.
14. قيس خلف صايل، أساليب الدعاية المستخدمة في مواقع الصحف الإلكترونية العراقية لتنمية الاستثمار المحلي، بحث منشور في مجلة لارك، العدد 2، المجلد 17، جامعة واسط — كلية الآداب، 2025. <https://doi.org/10.31185/lark.4161>
15. محمد أحمد سلامة مشعل، الحق في محو البيانات الشخصية، القاهرة، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، ج 3، ع 2، القاهرة، 2017.
16. مريم خالص حسين، الحكومة الالكترونية بحث منشور في مجلة كلية بغداد للعلوم الاقتصادية الجامعة، العدد الخاص بمؤتمر الكلية ، 2013.
17. ندى بدر جراح، الحكومة الالكترونية في العراق الواقع ومشاكل التطبيق في العراق، مجلة الخليج العربي، ع 3-4، 2012.

رابعا: الدساتير والقوانين

1. دستور جمهورية العراق لعام 2005.
2. الدستور المصري لسنة 2019.
3. الإعلان العالمي لحقوق الإنسان عام 1948 .
4. القانون المدني العراقي رقم 40 لسنة 1951.
5. قانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم 78 لسنة 2012.
6. قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018.
7. قانون حماية البيانات الشخصية المصري رقم 151 لعام 2020.
8. قانون حماية البيانات الشخصية الفرنسي رقم 801 لسنة 2004.

9. اللائحة الاوربية لحماية البيانات الشخصية رقم 679 لعام 2016 .
10. قانون الأحوال المدنية العراقي رقم (65) لسنة 1972 .
11. التوجيه الأوروبي لحماية البيانات لعام 2001.
12. قانون العقوبات العراقي رقم 111 لسنة 1969 النافذ.
13. قانون البطاقة الوطنية العراقي رقم (3) لسنة 2016 .
14. قانون العمل العراقي رقم 37 لسنة 2015.
15. قانون العمل العراقي الملغى رقم 71 لسنة 1987.
16. قانون العاملين بالدولة المصري رقم 47 لسنة 1978 .

خامساً: الروابط الإلكترونية

1-<https://www.un.org/ar/about-us/universal-declaration-of-human-rights>

2-<https://www.echr.coe.int/documents/d/echr/convention>

3-<https://www.coe.int/en/web/data-protection/convention>

4-<https://gdpr-info.eu/recitals>

5-<https://eur-lex.europa.eu/legal>

List of Sources

First: Books

1. Ahmed Abdelkarim Abu Shanab, Explanation of the Provisions of the Labor Law According to the Latest Amendments, 2nd ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, 2006.
2. Amal Qara, Criminal Protection of Information Technology in Algerian Legislation, 2nd ed., Dar Houma for Printing and Publishing, Algeria, 2007.
3. Salim Al-Jabouri, Legal Protection of Internet Network Information, Beirut, Al-Halabi Legal Publications, Beirut, 2011.
4. Atef Al-Naqeeb, The General Theory of Liability Arising from Personal Acts (Fault and Damage), Oweidat Publications, Lebanon, no publication date.
5. Abdelhamid Mohamed Al-Arabi, The Employee's Exercise of Public Freedoms in Administrative Law and International Law, no publication date.
6. Abdulaziz Al-Lasasmeh, Tort Liability for Harmful Acts, Dar Al-Ilmiya Publishing, Amman, 2002.
7. Abdulwadoud Yahya, Explanation of Labor Law, 3rd ed., Dar Al-Nahda Al-Arabiya, Cairo, 1989.
8. Ali Abdul-Fattah Muhammad Khalil, The Public Employee and the Practice of Political Freedom, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2002.
9. Majid Ragheb Al-Helou, Administrative Law, University Press, Alexandria, 1999. 10. Maher Saleh Al-Jubouri, Principles of Administrative Law, Baghdad, Legal Library, no publication date.
11. Muhammad Kamal Sharaf al-Din, Civil Law: General Theory, Persons, Proof of Rights, Official Press, Tunis, 2002.
12. Mustafa al-Jamal, Sources and Provisions of Obligation, Al-Halabi Legal Publications, Beirut, 2003.

Second: Theses and Dissertations

1. Ben Ashour, Saliha Ben Ashour, Inheritance and Bequest of Rights, PhD Dissertation, University of Algiers, 2007.
2. Abdelsalam Al-Awman, Criminal Protection of Personal Data in Jordanian Legislation, Master's Thesis, Middle East University, 2022.
3. Youssef Boujemaa, Protection of Personal Rights, Master's Thesis, University of Algiers, 2012.

Third: Research Papers

1. Ahmed Al-Awadat, Obstacles and Difficulties that Implement the E-Government Program, Amman, Irbid University, Journal of Economic and Administrative Sciences, Jordan, 2010.
2. Ahmed Qasim Al-Sudani, The Employee's Duty to Maintain Professional Secrecy: A Comparative Study, Journal of the Faculty of Law for Legal and Political Sciences. Volume 10, Issue 38, 2021.
3. Anwar Yahya, E-Government: Between Challenges and Risks, Beirut, Journal of E-Government: Between Challenges and Risks, Issue 20, 2015.
4. Hossam El-Din El-Ahwani, The Legal Protection of Privacy in the Face of Computers, Cairo, Ain Shams University, Journal of Legal and Economic Sciences, Issue 2, 1990.
5. Rizk Ali, Criminal Protection of Electronically Processed Personal Data in Light of Law No. 151 of 2020, Sadat University, Research Paper for the First Scientific Conference of the Faculty of Law at the University, 2022.
6. Sameh El-Tohamy, Controls for Processing Personal Data, Research Paper Published in the Proceedings of the International Conference, Kuwait International Law School, 2014.
7. Laila Ali Jumaa, Public Reliance on Social Media During Times of Crisis: The Dollar Exchange Rate Crisis as a Case Study, Research Paper Published in the Journal of Lark, Issue 5, Volume 14, Wasit University - College of Arts, 2022. <https://doi.org/10.31185/lark.Vol4.Iss47.2436>
8. Tariq Juma Rashid, "Legal Protection of Personal Data Privacy in the Digital Age," Journal of Law and Economics, No. 72, Cairo, 2019.
9. Alaa Hussein Al-Tamimi, "Public Utility Management under E-Government," Journal of the Arab Cultural Institute, Vol. 3, No. 3, Amman, 2007.
10. Fahd Mahmoud Al-Maamari, "E-Government," Muscat, Muscat Conference, Sultanate of Oman, 2010.
11. Qais Khalaf Sayel, "Advertising Methods Used on Iraqi Electronic Newspaper Websites to Develop Local Investment," research published in Lark Journal, Issue 2, Vol. 17, University of Wasit - College of Arts, 2025. <https://doi.org/10.31185/lark.4161>
12. Muhammad Ahmad Salama Mashal, "The Right to Erasure of Personal Data," Cairo, Journal of Legal and Economic Studies, Sadat University, Vol. 3, No. 2, Cairo, 2017.
13. Nada Badr Jarrah, "E-Government in Iraq: Reality and Implementation Problems in Iraq." Arabian Gulf Journal, Issues 3-4, 2012.

Fourth: Constitutions and Laws

1. Constitution of the Republic of Iraq of 2005.
2. Egyptian Constitution of 2019.

3. Universal Declaration of Human Rights of 1948.
4. Iraqi Civil Code No. 40 of 1951.
5. Electronic Signature and Electronic Transactions Law No. 78 of 2012.
6. Egyptian Cybercrime Law No. 175 of 2018.
7. Egyptian Personal Data Protection Law No. 151 of 2020.
8. French Personal Data Protection Law No. 801 of 2004.
9. European General Data Protection Regulation No. 679 of 2016.
10. Iraqi Civil Status Law No. (65) of 1972.
11. European General Data Protection Regulation (GDPR) 2001.
12. Iraqi Penal Code No. 111 of 1969 (in force).
13. Iraqi National Identity Card Law No. (3) of 2016.
14. Iraqi Labor Law No. 37 of 2015.
15. Repealed Iraqi Labor Law No. 71 of 1987.
16. Egyptian Civil Service Law No. 47 of 1978.

Fifth: Electronic Links

- 1-<https://www.un.org/ar/about-us/universal-declaration-of-human-rights>
- 2-<https://www.echr.coe.int/documents/d/echr/convention>
- 3-<https://www.coe.int/en/web/data-protection/convention>
- 5-[https:// : eur-lex.europa.eu/legal](https://eur-lex.europa.eu/legal)