



الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجا

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجا

أ.م.د. مهدي رجائي

أستاذ مساعد في كلية القانون / قسم القانون العام / جامعة قم - الجمهورية ايران الإسلامية.

Mahdi.Rajaei@gmail.com

علي احسان فتح الله

طالب الدكتوراه في القانون العام ، كلية القانون ، جامعة قم ، قم الجمهورية ايران الإسلامية.

Ali.Ihsan@gmail.com

الكلمات المفتاحية: الفجوة الرقمية - الضبط الإداري السيبراني - المشروعية الإدارية - النظام العام الرقمي - الحكومة الإلكترونية - القانون الإداري المقارن

كيفية اقتباس البحث

رجائي، مهدي ، علي احسان فتح الله ، الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجا، مجلة مركز بابل للدراسات الانسانية، تشرين الأول ٢٠٢٦، المجلد: ١٦، العدد: ١٠ .

هذا البحث من نوع الوصول المفتوح مرخص بموجب رخصة المشاع الإبداعي لحقوق التأليف والنشر (Creative Commons Attribution) تتيح فقط للآخرين تحميل البحث ومشاركته مع الآخرين بشرط نسب العمل الأصلي للمؤلف، ودون القيام بأي تعديل أو استخدامه لأغراض تجارية.

Registered في

ROAD

Indexed في

IASJ

The Digital Divide and Its Impact on the Legitimacy of Cybersecurity Administrative Control Egypt and Iraq as a Model

Asst. Prof. Dr. Mahdi Rajaei

Faculty of Law-Department of Public Law, University Of Qom , Islamic Republic of Iran.

Ali Ihsan Fathullah

PhD Candidate in Public Law, Faculty of Law, University of Qom, Qom, Islamic Republic of Iran

Keywords : Digital Divide – Cybersecurity Administrative Control – Administrative Legitimacy – Digital Public Order – E-Government – Comparative Administrative Law

How To Cite This Article

Rajaei, Mahdi, Ali Ihsan Fathullah, The Digital Divide and Its Impact on the Legitimacy of Cybersecurity Administrative Control Egypt and Iraq as a Model, Journal Of Babylon Center For Humanities Studies, October 2026, Volume:16, Issue 10.



This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

[This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.](http://creativecommons.org/licenses/by-nc-nd/4.0/)

Abstract:

This study addresses a nuanced and profound problem in contemporary administrative law: the impact of the digital divide on the legitimacy of cybersecurity administrative control in Egypt and Iraq. Administrative control traditionally derives its legitimacy from its ability to achieve its objectives of preserving public order and protecting rights. However, the digital divide threatens this legitimacy from two directions: it constrains the administration's capacity to fulfill its regulatory function in cyberspace, and simultaneously leads to disparities in cybersecurity protection levels across societal groups and state regions, thereby undermining the principles of equality before public services and the continuity of those services. The study concludes that addressing the digital divide is not an optional developmental requirement but a

necessary condition for achieving the legitimacy of cybersecurity administrative control, necessitating a comprehensive reform strategy at both the legislative and institutional levels. This research is divided into two complementary sections: the first addresses the nature of the digital divide and its impact on the legitimacy of cyber administrative regulation, while the second examines mechanisms to address this divide and enhance the legitimacy of administrative regulation at both the legislative and institutional levels.

The study concludes with a summary of the key findings and

المخلص:

تتناول هذه الدراسة إشكاليةً بالغة الدقة والعمق في مجال القانون الإداري المعاصر، تتمثل في الأثر الذي تحدثه الفجوة الرقمية على مشروعية الضبط الإداري السيبراني في كلٍّ من مصر والعراق. فالضبط الإداري يستمد مشروعيته تقليدياً من قدرته على تحقيق غاياته في صون النظام العام وحماية الحقوق، غير أن الفجوة الرقمية تُهدد هذه المشروعية من وجهيها: فهي تُقيد قدرة الإدارة على الاضطلاع بوظيفتها الضبطية في الفضاء السيبراني وتُفضي في الوقت ذاته إلى تفاوت في مستوى الحماية السيبرانية بين فئات المجتمع وأقاليم الدولة، مما يُخلّ بمبدأ المساواة أمام المرافق العامة ومبدأ استمرارية هذه المرافق. وتنتهي الدراسة إلى أن معالجة الفجوة الرقمية ليست مطلباً تنموياً اختيارياً بل شرطاً لازم لتحقيق مشروعية الضبط الإداري السيبراني وهو ما يستوجب استراتيجيةً إصلاحيةً شاملة على المستويين التشريعي والمؤسسي.

وتعتمد هذه الدراسة المنهج التحليلي النقدي المقارن الذي يجمع بين استقراء النصوص التشريعية وتحليل الواقع المؤسسي في البلدين، مع الاستناد إلى الفقه الإداري المقارن والمؤشرات الدولية للأمن السيبراني. وقد خلصت الدراسة إلى جملة من النتائج والتوصيات التي تُسهم في بناء تصورٍ إصلاحي لمنظومة الضبط الإداري السيبراني في السياق العربي. يُقسّم هذا البحث على مبحثين متكاملين؛ يتناول الأول ماهية الفجوة الرقمية وأثرها على مشروعية الضبط الإداري السيبراني، ويتناول الثاني آليات معالجة هذه الفجوة وتعزيز مشروعية الضبط الإداري على المستويين التشريعي والمؤسسي.

ونختتم الدراسة بخاتمة تتضمن أبرز النتائج والتوصيات.

المقدمة:

تُمثّل العلاقة بين الدولة والفضاء الرقمي إحدى أعمق الإشكاليات التي يواجهها القانون الإداري في القرن الحادي والعشرين؛ فالدولة التي بنى فقهاؤها وظائفها التقليدية على حفظ النظام العام في الفضاء المادي المحسوس تجد نفسها اليوم أمام فضاءٍ موازٍ لا مادي لا حدود جغرافية

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجاً

له ولا حضور جسدي فيه، وتجري فيه تفاعلات بالغة الأثر على مقومات الحياة الاجتماعية والاقتصادية للدول والأفراد. وهذا الفضاء الرقمي لم يُلغِ وظائف الإدارة العامة بل ضاعف من تعقيدها؛ إذ باتت البنى التحتية الحيوية للدولة من شبكات الكهرباء والمياه والمصارف والمستشفيات تعتمد اعتماداً شديداً كلياً على الأنظمة الرقمية، مما يعني أن أي خلل في هذا الفضاء ينعكس فوراً على الحياة المادية للمواطنين وعلى قدرة الدولة في الوفاء بالتزاماتها تجاههم.

وفي هذا السياق المتحول، يبرز مفهوم الضبط الإداري السيبراني بوصفه الامتداد الطبيعي للضبط الإداري التقليدي في بيئته الرقمية الجديدة؛ فكما يصون الضبط الإداري التقليدي النظام العام في الفضاء المادي عبر اللوائح والقرارات الإدارية، يصون الضبط الإداري السيبراني النظام العام الرقمي عبر السياسات المعلوماتية والتشريعات الرقمية وآليات الحماية التقنية. غير أن ما يُميّز هذا الضبط المستحدث عن سلفه التقليدي هو أنه يواجه تحدياً بنوياً فريداً لم يعرفه الضبط الإداري التقليدي: إنه يُمارَس في ميدان تهيم على بنيته التحتية شركات خاصة لا جهات حكومية، ويستلزم كفاءات تقنية متخصصة نادراً ما تمتلكها الأجهزة الإدارية بالقدر الكافي، وتتجاوز تهديداته الحدود الجغرافية التي تقوم عليها السيادة الوطنية.

وتأتي الفجوة الرقمية لتضيف إلى هذه التعقيدات طبقةً أخرى من الإشكاليات؛ فهي تعني في أبسط تعريفاتها التفاوت في القدرة على الوصول إلى التكنولوجيا الرقمية وتوظيفها، غير أنها في السياق الإداري الذي تتناوله هذه الدراسة تحمل معنىً أعمق وأشد خطورة: إنها تعني عجز الإدارة العامة ذاتها عن مجاراة الفضاء الرقمي الذي تُكَلَّف بضبطه وصونه. فالدولة التي تمتلك تشريعات سيبرانية متقدمة لكنها تفتقر إلى البنية التقنية والكوادر البشرية والتنسيق المؤسسي اللازم لتطبيقها تمتلك في الحقيقة مشروعيةً شكليةً لا تُترجم إلى ضبط فعلي. وهذه المفارقة بين النص والواقع، بين الطموح التشريعي والقدرة المؤسسية، هي ما تُجسِّد الفجوة الرقمية في أعماق أبعادها القانونية، وهو ما يدفع هذه الدراسة إلى التساؤل عن الأثر الذي تُحدثه هذه الفجوة على مشروعية الضبط الإداري السيبراني في تجربتي مصر والعراق.

أهمية الدراسة

تتجلى أهمية هذه الدراسة على صعيدين نظري وعملي، على الصعيد النظري، تُقدِّم هذه الدراسة إسهاماً في بناء نظرية قانونية إدارية متكاملة لمفهوم المشروعية الغائية للضبط الإداري السيبراني؛ وهو مفهوم لا يزال يفتقر إلى تأصيل فقهي عربي وافٍ يربط بين الفجوة الرقمية من جهة ومبادئ القانون الإداري الراسخة كاستمرارية المرفق العام والمساواة أمامه والمشروعية

الإجرائية من جهة أخرى. وتتنبثق الأهمية النظرية أيضاً من كون هذه الدراسة تتناول الضبط الإداري السيبراني بوصفه امتداداً طبيعياً للنظرية العامة للضبط الإداري لا انفصلاً عنها، وهو ما يُعيد طرح أسئلة فلسفية جوهرية حول قدرة المفاهيم القانونية الكلاسيكية على استيعاب التحولات الرقمية دون أن تفقد تماسكها النظري. فضلاً عن ذلك، تُسهم الدراسة في إثراء الأدبيات القانونية المقارنة من خلال تقديم قراءة نقدية لتجربتين عربيتين متباينتين في درجة نضجها المؤسسي والتشريعي السيبراني، مما يُوفر نموذجاً مقارناً قابلاً للتعميم على سياقات عربية مشابهة.

وعلى الصعيد العملي، تكتسب هذه الدراسة أهمية استثنائية في ضوء الرهانات التنموية والأمنية التي تواجهها مصر والعراق في مسيرتهما نحو التحول الرقمي الحكومي. فمصر التي أطلقت استراتيجيتها الوطنية للأمن السيبراني (٢٠٢٣-٢٠٢٧) وتسعى إلى تعزيز موقعها في المؤشرات الدولية، والعراق الذي يُعيد بناء بنيته المؤسسية الرقمية في ظل تحديات أمنية وسياسية متراكمة، يحتاجان إلى قراءة قانونية موضوعية تكشف الثغرات وتُقدّم المعالجات ضمن إطار القانون الإداري المقارن لا خارجه. وتتجلى الأهمية العملية كذلك في أن نتائج هذه الدراسة وتوصياتها تُخاطب بشكل مباشر صانعي القرار التشريعي والإداري في البلدين، إذ تُقدّم لهم خارطة طريق قانونية مستندة إلى تحليل مقارن رصين تُحدد الأولويات وتُرتبها وفق منطق القانون الإداري لا منطق التقنية وحدها. وفي هذا السياق، يُمثّل هذا البحث رافداً علمياً لجهود التشريع السيبراني المقبلة في العراق الذي يقف اليوم على عتبة مرحلة تأسيسية حاسمة في بناء منظومته القانونية الرقمية.

إشكالية الدراسة

إن المتأمل في واقع الضبط الإداري السيبراني في مصر والعراق يجد تناقضاً لافت يستعصي على التفسير السطحي، فكل البلدان يمتلكان إرادة سياسية معلنة في تعزيز أمنهما السيبراني، ويمتلكان تشريعات ذات صلة، وتوجد فيهما جهات إدارية تدّعي الاختصاص بهذا الشأن. غير أن مؤشرات الجاهزية السيبرانية الدولية تكشف عن هشاشة واضحة في منظومة الضبط الإداري السيبراني في العراق وعن قصور في التطبيق الفعلي في مصر رغم تقدمها النسبي. وهذا التناقض بين الإرادة والأداء، بين النص والواقع، بين الطموح والقدرة، يُشير إلى عامل هيكلي خفي يُشوّه فاعلية منظومة الضبط ويُقيّد مشروعيتها الغائية. وهذا العامل الخفي هو ما تُسمّيه هذه الدراسة الفجوة الرقمية بمعناها الإداري الشامل الذي يتجاوز مجرد التفاوت في الأجهزة والشبكات ليُطال القدرة المؤسسية والبشرية والتشريعية على إدارة الفضاء الرقمي وضبطه.

ومن هذا المنطلق، يدور هذا البحث حول سؤال مركزي واحد:

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجاً

هل تُفضي الفجوة الرقمية بأبعادها التقنية والبشرية والمؤسسية إلى إخلال بمشروعية الضبط الإداري السيبراني في مصر والعراق؟ وما السبيل إلى معالجة هذه الفجوة لاستعادة المشروعية الكاملة لهذا الضبط؟

ويتفرع عن هذا السؤال المركزي جملةً من الأسئلة الفرعية التي تُشكّل في مجموعها خريطة البحث ومحاور إجابته:

- ما المقصود بالفجوة الرقمية في السياق الإداري، وكيف تتجلى في التجريبتين المصرية والعراقية؟
- هل يُخلّ التفاوت في مستوى الحماية السيبرانية بين المناطق والجهات الإدارية بمبدأ المساواة أمام المرافق العامة؟
- كيف تُهدد الفجوة الرقمية مبدأ استمرارية المرفق العام في الفضاء السيبراني؟
- ما الشروط التشريعية والمؤسسية اللازمة لتجاوز هذه الفجوة وتعزيز مشروعية الضبط الإداري السيبراني؟

منهجية الدراسة

تعتمد هذه الدراسة المنهج التحليلي النقدي المقارن؛ إذ تُحلّل النصوص التشريعية وتُقيّمها نقدياً في ضوء الواقع التطبيقي، وتُقارن بين التجريبتين المصرية والعراقية مستعيناً بالفقه الإداري المقارن والمؤشرات الدولية للأمن السيبراني.

هيكلية الدراسة

يُقسّم هذا البحث على مبحثين متكاملين؛ يتناول الأول ماهية الفجوة الرقمية وأثرها على مشروعية الضبط الإداري السيبراني، ويتناول الثاني آليات معالجة هذه الفجوة وتعزيز مشروعية الضبط الإداري على المستويين التشريعي والمؤسسي. ونختتم الدراسة بخاتمة تتضمن أبرز النتائج والتوصيات.

المبحث الأول

ماهية الفجوة الرقمية وأثرها على مشروعية الضبط الإداري السيبراني

لا يمكن فهم الأثر الذي تُحدثه الفجوة الرقمية على مشروعية الضبط الإداري السيبراني دون استيعاب المفهومين الجوهريين اللذين يقوم عليهما هذا البحث؛ مفهوم الفجوة الرقمية بأبعادها المتشعبة، ومفهوم مشروعية الضبط الإداري السيبراني بمعناه الموسّع الذي يتجاوز المشروعية الشكلية القائمة على النص التشريعي وحده. وعلى هذا الأساس، يُقسّم هذا المبحث على مطلبين؛

الأول لدراسة الفجوة الرقمية ومستوياتها، والثاني لتحليل أثرها على مشروعية الضبط الإداري في التجريبتين المصرية والعراقية.

المطلب الاول

مفهوم الفجوة الرقمية وأبعادها في السياق الإداري

لا يمكن الإمساك بالأثر الذي تحدثه الفجوة الرقمية على منظومة الضبط الإداري السيبراني دون البدء بتأسيس مفهومي دقيق يُحرّر هذه الظاهرة من تعريفاتها الاقتصادية والتنموية السائدة ليُعيد قراءتها من منظور القانون الإداري. فالفجوة الرقمية في أدبيات التنمية تُوصف عادةً بأنها تفاوت في إمكانية الوصول إلى تكنولوجيا المعلومات والاتصالات بين الأفراد والمجتمعات، وهو تعريف صحيح في حدوده لكنه قاصر في سياق هذه الدراسة التي تتناول الجهاز الإداري لا الفرد المواطن. فالفجوة الرقمية التي يعنيها القانون الإداري هي تلك التي تُصيب الإدارة العامة في قدرتها الضبطية؛ أي الهوة بين ما تستلزمه وظيفة الضبط الإداري في الفضاء السيبراني من موارد وكفاءات ومؤسسات، وما تمتلكه الإدارة فعلاً من هذه المقومات. وهذه الهوة ليست واحدة في طبيعتها بل تتعدد مستوياتها وتتشابك أبعادها، وهو ما يستدعي دراستها في فرعين؛ يتناول الأول تعريف الفجوة الرقمية، ويتناول الثاني مظاهرها الملموسة في التجريبتين المصرية والعراقية.

الفرع الأول

تعريف الفجوة الرقمية

لا يمكن الإمساك بجوهر الفجوة الرقمية في سياقها الإداري القانوني إذا اكتفى بتعريفها الاقتصادي والتنموي المتداول الذي يُصوّرها تفاوتاً في الحصول على الأجهزة والشبكات؛ فهذا التعريف وإن كان صحيحاً في نطاقه إلا أنه يُخفي البُعد الأعرق الذي يعنيه القانون الإداري حين يتناول هذه الظاهرة. فالفجوة الرقمية في المجال الإداري هي في جوهرها فجوة في القدرة الضبطية؛ أي الهوة بين ما تستلزمه وظيفة الضبط الإداري في الفضاء السيبراني من إمكانات تقنية وبشرية ومؤسسية، وما تمتلكه الإدارة العامة فعلاً من هذه الإمكانيات. وهذا التعريف يُنقل الفجوة الرقمية من حقل التنمية الاقتصادية إلى صميم القانون الإداري المقارن، ويجعلها مسألة تتعلق بمشروعية الضبط لا بالتخلف التقني وحده^(١).

أولاً: الفجوة الرقمية بين التعريف التنموي والتعريف الإداري

ظلّ مفهوم الفجوة الرقمية حكراً على أدبيات التنمية والاقتصاد الرقمي زمناً طويلاً، قبل أن يشقّ طريقه إلى حقل القانون الإداري المقارن. ففي أدبيات التنمية، تُعرّف الفجوة الرقمية بأنها "التفاوت في إمكانية الوصول إلى تكنولوجيا المعلومات والاتصالات بين الأفراد والمجتمعات

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجاً

والدول"، وهو تعريف يُركّز على البُعد الكمي المتمثل في امتلاك الأجهزة والاتصال بالشبكات. أما في السياق الإداري القانوني الذي نتناوله هذه الدراسة، فالفجوة الرقمية تعني شيئاً أكثر تعقيداً وأبعد أثراً؛ إنها تعني التفاوت في القدرة الضبطية للإدارة العامة في الفضاء السيبراني، بما يشمل قدرتها على مراقبة هذا الفضاء وتنظيمه والاستجابة للتهديدات التي تطاله^(٢).

وقد أسهمت الدراسات الأكاديمية المتخصصة في التحول الرقمي للإدارة العامة في إمطة اللثام عن هذا البُعد القانوني المُهمَل للفجوة الرقمية؛ إذ كشفت هذه الدراسات أن التحول الرقمي في الإدارة العامة يستلزم تكاملاً بين ثلاثة جوانب متلازمة: الجانب التقني المتمثل في البنية التحتية الرقمية، والجانب البشري المتمثل في الكوادر المؤهلة، والجانب القانوني المتمثل في الإطار التشريعي والمؤسسي الناظم. وغياب أيٍّ من هذه الجوانب يُؤلّد فجوةً رقميةً حتى وإن توافر الجانبان الآخران، مما يعني أن الفجوة الرقمية ظاهرةً متعددة الأبعاد لا يُعالجها حلٌّ أحادي^(٣).

ثانياً: مستويات الفجوة الرقمية في الجهاز الإداري

يُميّز الفقه الإداري المعاصر بين ثلاثة مستويات مترتبة للفجوة الرقمية في الجهاز الإداري تتشابه فيما بينها دون أن يُغني أحدها عن الآخر في التشخيص:

المستوى الأول - فجوة البنية التحتية: تعني ضعف الأنظمة الرقمية الحكومية وهشاشتها أمام التهديدات السيبرانية. وتتجلى هذه الفجوة في قصور الأنظمة الحكومية وعدم استيفائها الحد الأدنى من متطلبات الأمن السيبراني، مما يجعل الأجهزة الإدارية تعمل على منصات رقمية هشة لا تُوفر الحماية الكافية للمعاملات والبيانات الحكومية. وقد وثّق تقرير الاتحاد الدولي للاتصالات لعام ٢٠٢٣ تدني مؤشرات العراق في الجاهزية السيبرانية مقارنةً بدول الجوار، حيث لم تتجاوز نسبة تقييمه ٢٠% في مؤشرات الأمن السيبراني العالمي، بما يعني أن الأجهزة الإدارية تعمل على منصات رقمية لا تستوفي الحد الأدنى من متطلبات الأمن السيبراني^(٤).

المستوى الثاني - فجوة الكوادر البشرية: تعني ندرة الكفاءات المتخصصة في أمن المعلومات داخل الجهاز الإداري. ويُعزى ذلك في الغالب إلى ضعف برامج التدريب والتأهيل وعدم قدرة الإدارة على المنافسة مع القطاع الخاص في استقطاب الكفاءات نظراً لفوارق الرواتب والحوافز. وتكشف الدراسات الميدانية أن ٧٢% من موظفي الجهات الحكومية لا يمتلكون أدنى معرفة بسياسة أمن المعلومات في مؤسساتهم، وأن ٧٤% لم يتلقوا أي تدريب منظم على الأمن السيبراني^(٥). وهذه الأرقام تُجسّد الخطر الحقيقي للفجوة البشرية؛ فالموظف غير المُدرَّب يتحول من عنصر حماية إلى نقطة ضعف في المنظومة الضبطية بأكملها.

المستوى الثالث - فجوة المؤسسة: تعني غياب الهيكل المؤسسي الرقابي القادر على تنسيق جهود الضبط الإداري السيبراني بين الجهات المتعددة وضمان اتساقها. وهذه الفجوة هي الأشد خطورةً من المنظور القانوني الإداري لأنها تُقضي إلى تشتت الاختصاص السيبراني؛ إذ تتعدد الجهات التي تدّعي صلاحية الضبط الإداري في الفضاء الرقمي دون أن يُحدد تشريع واضح حدود كل منها، مما يُولّد تعارضاً في التطبيق وفراغاً في المساءلة^(٦).

ثالثاً: التمييز بين نوعي الفجوة الرقمية وأثره على منظومة الضبط

يُضيف الفقه الإداري في هذا السياق تمييزاً دقيقاً بالغ الأهمية بين نوعين من الفجوة الرقمية: فجوة الوصول التي تعني غياب البنية التحتية التقنية أو صعوبة الحصول عليها، وفجوة الاستخدام التي تعني العجز عن توظيف التقنية المتاحة بكفاءة حتى حين تتوافر. وما يلاحظ في كلٍّ من مصر والعراق أن الإشكالية لا تقتصر على فجوة الوصول بل تجمع النوعين معاً؛ فالإدارة أحياناً تمتلك الأجهزة لكن لا تمتلك الكفاءة البشرية لتشغيلها أمنياً، وتمتلك الشبكة لكن لا تمتلك البروتوكولات الكافية لحمايتها^(٧).

وهذا التضافر بين الفجوتين يُنتج ما يمكن تسميته الفجوة المركبة التي تُعاني منها معظم الأجهزة الإدارية في الدول النامية، وهي فجوة تستعصي على المعالجة الجزئية وتستلزم استراتيجية شاملة تُعالج الأبعاد التقنية والبشرية والمؤسسية في آنٍ واحد. والجدير بالإشارة أن الفقه الإداري المقارن يذهب إلى أن هذه الفجوة المركبة تُولّد مسؤولية إدارية مُضاعفة على الدولة؛ إذ لا يكفي أن تُصدر الدولة تشريعات سيبرانية متقدمة، بل يقع عليها التزام قانوني بتوفير البنية الموضوعية اللازمة لتطبيقها، وإلا وقعت في تناقض يُخلّ بمبدأ التسلسل الهرمي للالتزامات القانونية الإدارية^(٨).

رابعاً: الفجوة الرقمية وأزمة مشروعية الضبط

وإذا كانت الفجوة الرقمية بمستوياتها الثلاثة تُعيق قدرة الإدارة على أداء وظيفتها الضبطية، فإنها تُثير في الوقت ذاته سؤالاً مفاده: هل يمكن مساءلة الإدارة عن التقصير في الضبط الإداري السيبراني حين تفتقر أصلاً إلى الأدوات اللازمة للوفاء بالتزاماتها في هذا المجال؟ وهذا السؤال يكشف عن توتر جوهري في القانون الإداري بين مبدئين قانونيين متناقضين في ظاهرهما: مبدأ المسؤولية الذي يُلزم الإدارة بالوفاء بواجباتها الضبطية تحت طائلة المساءلة، ومبدأ التكليف بما لا يُطاق الذي يقتضي ألا تُكَلّف الإدارة بالتزامات تتجاوز قدرتها الفعلية. والإجابة الصحيحة عن هذا التوتر لا تكمن في الإعفاء من المسؤولية بل في فرض التزام مضاعف: التزام بتعزيز

القدرات المؤسسية التقنية والبشرية بالتوازي مع الالتزام بممارسة الضبط ضمن حدود ما هو متاح^(٩).

الفرع الثاني

مظاهر الفجوة الرقمية

لا تتجلى الفجوة الرقمية بالصورة ذاتها في كل التجارب الإدارية؛ فهي تتلون بحسب السياق التاريخي والمؤسسي لكل دولة وتتفاوت في حدتها وطبيعتها بين تجربة وأخرى. ومن هنا تكتسب المقارنة بين التجريبتين المصرية والعراقية قيمةً تحليليةً استثنائيةً؛ فهما تجربتان تنتميان إلى السياق العربي ذاته وتواجهان تحديات بنىوية متشابهة، لكنهما تقفان في مواقع متباينة على طيف الجاهزية السيبرانية، مما يجعل مقارنتهما أداةً تحليليةً قادرةً على الكشف عن الأنماط المؤسسية والتشريعية التي تُحدد مسار هذه الفجوة ومآلاتها.

أولاً: مظاهر الفجوة الرقمية في التجربة المصرية

لا يمكن وصف التجربة المصرية في مجال الأمن السيبراني بأنها تجربة تعاني من الفجوة الرقمية بمعناها الكلاسيكي المتمثل في ضعف البنية التحتية أو غياب التشريع؛ فمصر أحرزت تقدماً مؤشراً في هذا المجال وصل إلى حد تصنيفها ضمن المستوى الأول في مؤشر الأمن السيبراني العالمي (GCI) لعام ٢٠٢٤ بدرجة كاملة ١٠٠ نقطة، لتصبح ضمن أفضل ١٢ دولة أداءً على مستوى العالم وتحتل المركز الأول إفريقياً في مجال الأمن السيبراني^(١٠). وقد انعكس هذا التقدم على مساهمة قطاع الاتصالات وتكنولوجيا المعلومات في الناتج المحلي الإجمالي التي ارتفعت من ٣% عام ٢٠١٣ إلى ٥.٨% عام ٢٠٢٤^(١١).

غير أن هذه المؤشرات الإيجابية لا تعني انعدام الفجوة الرقمية بل تعني تحولها من فجوة الوصول إلى ما يمكن تسميته فجوة الاتساق المؤسسي؛ وهي فجوة أشد دقةً وأصعب تشخيصاً. ففي ظل وجود الإطار التشريعي والمؤسسي، تبقى الفجوة الرقمية المصرية متجليةً في ثلاثة مظاهر رئيسية: أولها التفاوت الجغرافي في مستوى الحماية السيبرانية بين المحافظات الكبرى والمناطق النائية؛ إذ لا تزال المحافظات الحدودية والصعيد تعاني من ضعف في جودة خدمات الاتصالات مما يُقيد قدرة الإدارات المحلية على الانخراط في منظومة الضبط الإداري الرقمي الوطنية. وثانيها الفجوة بين التشريع والتطبيق التي تتجلى في أن الهجمات السيبرانية على الجهات الحكومية المصرية بلغت ٣٨ مليون هجمة عام ٢٠٢٤ مقارنةً بـ ١٣ مليون هجمة عام ٢٠٢٣، وهو رقم يكشف أن الإطار التشريعي المتقدم لم يُترجم بعد إلى حصانة سيبرانية كاملة^(١٢). وثالثها قصور التنسيق المؤسسي بين الجهات المتعددة المعنية بالأمن السيبراني،

وهو ما يعكسه ما أوصى به مجلس الشيوخ المصري من ضرورة تعزيز الأطر التنظيمية وتنظيم محاكاة للتهديدات السيبرانية داخل المؤسسات.

ثانياً: مظاهر الفجوة الرقمية في التجربة العراقية

تُجسّد التجربة العراقية نموذجاً مغايراً تماماً للفجوة الرقمية؛ فهي لا تعاني من فجوة الاتساق المؤسسي كنظيرتها المصرية بل تعاني من الفجوة البنيوية الشاملة التي تطال كل مستويات المنظومة الإدارية الرقمية. وتكشف المؤشرات الدولية حجم هذه الهوة بأرقام صريحة؛ إذ جاء العراق في المرتبة ١٣٤ عالمياً من أصل ١٩٤ دولة في مؤشر الأمن السيبراني العالمي (GCI) بنسبة ٥٣% في الفئة الرابعة، وهو ترتيب يضعه ضمن أضعف عشر دول في منطقة الشرق الأوسط وشمال أفريقيا من حيث النضج السيبراني^(١٣). (٤) بل يذهب أبعد من ذلك في مؤشر جاهزية الشبكة (NRI) لعام ٢٠٢٤ إذ خرج العراق من التصنيف العالمي كلياً في حين شمل المؤشر ١٣٣ دولة^(١٤).

وتتجلى مظاهر الفجوة الرقمية في العراق في أربعة محاور: أولها إرث البنية التحتية الهشة الذي يجد جذوره في عقود من الحروب والحصار الاقتصادي والاضطرابات السياسية التي حالت دون تطوير بنية رقمية حكومية متينة؛ فالجهاز الإداري العراقي ورث بنيةً تحتيةً معلوماتيةً ضعيفة لا تستوفي الحد الأدنى من متطلبات الأمن السيبراني وهو ما تراكم عبر عقود لا يمكن تجاوزه بقرارات آنية^(١٥). وثانيها الجمود المنهجي في الاستراتيجية الوطنية إذ تمتد الخطة الحالية على تصورات تعود إلى عقد سابق ولا تعكس بشكل كافٍ التحولات الحديثة في مجالات الحوكمة السيبرانية والذكاء الاصطناعي وحروب البيانات^(١٦). وثالثها فجوة الحوكمة التي تتجلى في محدودية تطبيق أطر إدارة المخاطر والامتنال مما يُضعف قدرة المنظومة السيبرانية على فرض معايير أمنية موحدة على مستوى الدولة^(١٧). ورابعها التشتت المؤسسي بين وزارة الداخلية والأمن الوطني وهيئة الاتصالات والإعلام والجهات الأمنية المختلفة، دون جهة مرجعية موحدة تنسق جهودها وتوجّهها^(١٨).

تكشف المقارنة بين المظهرين عن ثلاث نتائج تحليلية ذات أثر مباشر في سياق هذه الدراسة: **النتيجة الأولى:** الفجوة الرقمية ليست ظاهرةً ثنائيةً (موجودة أو غائبة) بل هي طيفٌ متدرج تقع الدول في نقاط مختلفة منه. فمصر والعراق كلتاهما تعانيان من الفجوة الرقمية، لكن بأشكال ومستويات متفاوتة تستلزم استجابات إصلاحية مختلفة.

النتيجة الثانية: التقدم في المؤشرات الدولية لا يعني انعدام الفجوة الرقمية بل يعني تحوّلها من شكل إلى آخر. فمصر التي تصدر المؤشرات العالمية تعاني من فجوة التطبيق والاتساق، في

حين يعاني العراق من فجوة البناء والتأسيس. والاثنتان تُخلّان بمشروعية الضبط الإداري السيبراني وإن اختلف وجه الإخلال^(١٩).

النتيجة الثالثة: كلتا الفجوتين ترتبان على الدولة التزامات قانونية إدارية مختلفة في طبيعتها؛ فمصر مُلزَمة بتعميق الإصلاح وردم فجوة التطبيق، في حين يقع على العراق التزام تأسيسي ببناء المنظومة من قواعدها الأولى. وهذا التمييز القانوني بين نوعي الالتزام هو ما يُشكّل مدخل الفصل القادم في تحليل السبل الكفيلة بمعالجة الفجوة الرقمية في كلا البلدين.

المطلب الثاني

أثر الفجوة الرقمية على مشروعية الضبط الإداري السيبراني

في فلسفة القانون الإداري المقارن، لا تنحصر مشروعية الضبط الإداري في استيفاء شروطه الشكلية من اختصاص وإجراءات وأسباب؛ فهذه الشروط وإن كانت ضرورية إلا أنها لا تكفي وحدها لمنح الضبط مشروعيته الكاملة. ذلك أن الضبط الإداري يستمد جزءاً جوهرياً من مشروعيته من قدرته الفعلية على تحقيق الغايات التي أسّس من أجلها؛ فضبط يُقرّه النص ولا تُنفّذه الإدارة، أو تُنفّذه بعجز يُخلّ بفاعليته، أو تُطبّقه بتفاوت يُخلّ بعدالته، هو ضبط مُختلّ في مشروعيته الغائية حتى وإن كان سليماً في مشروعيته الشكلية. وهذا التمييز بين مستويي المشروعية هو ما يمنح الفجوة الرقمية أثراً قانونياً حقيقياً يتجاوز كونها ظاهرة تقنية أو تنموية. فحين تعجز الإدارة العامة عن أداء وظيفتها الضبطية في الفضاء السيبراني بسبب ضعف بنيته التقنية أو قصور كوادرها البشرية أو تشتت اختصاصاتها المؤسسية، لا تكون هذه المشروعية الغائية متحققة حتى وإن توافرت النصوص التشريعية الكافية. وهذا الخلل في المشروعية يتجلى تحديداً في مسّ الفجوة الرقمية لمبدأين راسخين في القانون الإداري لا تقوم الإدارة الحديثة بدونهما: مبدأ استمرارية المرفق العام ومبدأ المساواة أمامه، فضلاً عن إحداثها ما يمكن تسميته فجوة التطبيق التشريعي التي تُفرغ النص التشريعي من قدرته الإلزامية. وهذان الوجهان من وجوه الخلل في المشروعية هما ما يتناولهما هذا المطلب في فرعيه.

الفرع الأول

الاخلال بمبدأ استمرارية المرفق العام ومبدأ المساواة

عدّ مبدأ استمرارية المرفق العام من أعرق المبادئ التي أرساها القانون الإداري الفرنسي وتبنّتها الأنظمة القانونية العربية المقارنة؛ فهو يقتضي أن تؤدي المرافق العامة خدماتها بصورة منتظمة ومستمرة دون انقطاع، لأن في الانقطاع إخلالاً بالالتزام الجوهري للدولة تجاه مواطنيها. وقد كان هذا المبدأ في أصله التاريخي يعالج إشكاليات الإضراب وتوقف الموظفين عن العمل والكوارث

الطبيعية بوصفها أسباباً لانقطاع المرفق، غير أن الثورة الرقمية أضافت إلى قائمة هذه الأسباب عاملاً لم يتوقعه المؤسسون: الاختراق السيبراني وتعطل الأنظمة الرقمية الحكومية^(٢٠). وهنا يبرز السؤال التالي: هل الفجوة الرقمية التي تجعل الأنظمة الحكومية عرضة للاختراق والتعطيل تُعد انتهاكاً لمبدأ استمرارية المرفق العام قبل وقوع الاختراق، أم أن الانتهاك لا يتحقق إلا بعد وقوعه فعلاً؟

أولاً: الفجوة الرقمية وانتهاك مبدأ الاستمرارية

يذهب الفقه الإداري الحديث إلى أن مبدأ استمرارية المرفق العام لا يقتصر في مفهومه على منع الانقطاع الفعلي، بل يمتد ليشمل واجب الإدارة في اتخاذ التدابير الوقائية اللازمة للحيلولة دون الانقطاع المحتمل. وبهذا المفهوم الموسع، تُشكل الفجوة الرقمية انتهاكاً استباقياً لمبدأ الاستمرارية؛ إذ إن إدارة تُشغل أنظمة رقمية هشة لا تستوفي معايير الأمن السيبراني الأدنى تُعرض استمرارية مرافقها للخطر بصورة منهجية لا عارضة^(٢١). وقد كشفت حادثة اختراق موقع جهاز مكافحة الإرهاب العراقي عام ٢٠١٩ والترويج لبيان مزيف عن انقلاب عسكري أن الفجوة الرقمية لم تكن مجرد تقصير تقني بل كانت سبباً مباشراً في اهتزاز الثقة بالمرافق العام وتعطيل أدائه الاتصالي الجوهري^(٢٢). ويتعمق هذا الأثر حين ندرك أن المرافق العامة في العصر الرقمي باتت مترابطة ترابطاً عضوياً بحيث يُفضي تعطل أيٍّ منها إلى تسلسل من التعطلات في المرافق المترابطة؛ فاختراق منظومة الاتصالات الحكومية يُشَلّ التنسيق بين المرافق الأخرى، واختراق المنظومة المصرفية يُعطل المدفوعات الحكومية، واختراق قواعد بيانات الهوية يُوقف الخدمات المدنية. وهذا الترابط يجعل الفجوة الرقمية في أي حلقة من حلقات المنظومة تهديداً لاستمرارية المنظومة بأكملها، لا لمرفق بعينه^(٢٣). وقد أشارت دراسة لمجلس الشيوخ المصري إلى أن الهجمات الإلكترونية على الجهات الحكومية المصرية بلغت ٣٨ مليون هجمة عام ٢٠٢٤، وهو رقم يُجسّد حجم التهديد الذي تُواجهه استمرارية المرافق العامة الرقمية في ظل الفجوة الرقمية القائمة.

ثانياً: الفجوة الرقمية والإخلال بمبدأ المساواة أمام المرافق العامة

يُعدّ مبدأ المساواة أمام المرافق العامة من المبادئ الدستورية التي أرسى القضاء الإداري المقارن معالمها بوضوح؛ فهو يقتضي أن يتلقى المواطنون الخدمة العامة بمستوى متكافئ دون تمييز على أساس الموقع الجغرافي أو الانتماء الاجتماعي أو الانتماء المؤسسي. وتُمثّل الفجوة الرقمية انتهاكاً صريحاً لهذا المبدأ من منظور مزدوج: منظور المواطن الذي يتفاوت مستوى الحماية السيبرانية التي تُوفرها له الإدارة تبعاً لموقعه الجغرافي، ومنظور المؤسسة الإدارية ذاتها

التي تتفاوت قدرتها على الضبط السيبراني بين وزارة وأخرى وبين محافظة وأخرى^(٢٤). وتتجلى هذه اللامساواة في التجربة العراقية بشكل حاد؛ إذ تتركز قدرات الضبط الإداري السيبراني في المركز وتشحّ في المحافظات البعيدة، مما يعني أن المواطن في المحافظات النائية يحصل على خدمة عامة رقمية أقل أماناً وأضعف حمايةً من نظيره في بغداد دون أي مسوّغ قانوني لهذا التمييز. وهذا التفاوت في الحماية السيبرانية يُعيد إنتاج اللامساواة الاجتماعية بصورة جديدة؛ فالمناطق الأكثر هشاشة اجتماعياً وتنموياً هي ذاتها الأكثر انكشافاً سيبرانياً، مما يُضاعف التهميش ويُرسّخ الفجوة التنموية الأصلية تحت غطاء رقمي^(٢٥).

أما على الصعيد المصري، فتبرز لا المساواة في شكل مختلف يتعلق بالتفاوت في مستوى الاستجابة السيبرانية بين الجهات الحكومية المختلفة؛ فالوزارات والهيئات ذات الطابع السيادي تحظى ببنية سيبرانية أفضل مما تحظى به الإدارات المحلية والهيئات الخدمية، مما يعني أن المواطن الذي يتعامل مع الإدارة المحلية يخضع لمستوى أدنى من الحماية السيبرانية مقارنةً بمن يتعامل مع الجهات المركزية. وهذا التفاوت يُخلّ بمبدأ المساواة أمام المرافق العامة لأنه يجعل درجة الحماية التي يتمتع بها المواطن رهينةً بطبيعة الجهة التي يتعامل معها لا بحقه الوصول في الحماية المتكافئة^(٢٦).

ثالثاً: التوتر بين الاستمرارية والمساواة والأمن السيبراني

ويكشف التحليل المعمّق لأثر الفجوة الرقمية على المبدئين عن توتر ثلاثي دقيق لا يُعالجه البحث القانوني الكلاسيكي بالقدر الكافي؛ فمحاولة الإدارة سدّ الفجوة الرقمية وتعزيز أمنها السيبراني قد تُفضي في حالات معينة إلى تعارض مؤقت بين متطلبات الأمن والاستمرارية والمساواة في آنٍ واحد. فتقييد الوصول إلى بعض الأنظمة لأسباب أمنية قد يُقيّد استمراريته مؤقتاً، وتخصيص موارد محدودة لتأمين الأنظمة الأكثر حساسية قد يُفضي إلى تفاوت في الحماية يمسّ مبدأ المساواة. وهذا التوتر يستوجب تأطيراً قانونياً دقيقاً يُحدد الأولويات ويُقرّر المفاضلة المشروعة بين هذه المبادئ في ضوء مبدأ التناسب الذي يُعدّ الحكم الأمثل لهذه المفاضلات في القانون الإداري المقارن^(٢٧).

الفرع الثاني

فجوة التطبيق التشريعي وأثرها على المشروعية الغائبة

يُطرح في هذا الفرع مفهوم قانوني مُستحدث الى حد ما، وهو مفهوم فجوة التطبيق التشريعي الذي يُعبّر عن الهوة بين ما تتضمنه النصوص التشريعية من التزامات وحقوق في مجال الأمن السيبراني، وما يُمكن تحقيقه فعلاً في ظل غياب البنية التقنية والبشرية اللازمة لتطبيقها. وما

يجعل هذه الفجوة إشكالية قانونية حقيقية لا مجرد قصور تقني هو أنها تُخلّ بما يُسميه الفقه الإداري الحديث المشروعية الغائية للتشريع؛ فالتشريع الذي يُقرّر حقوقاً لا يمكن استيفاؤها يُعلن مشروعية شكلية لكنه يُنتج عجزاً موضوعياً، ويُوجد التزاماً لفظياً دون أن يُفضي إلى أثر قانوني فعلي.

أولاً: مفهوم فجوة التطبيق التشريعي وشروط تحققها

تتحقق فجوة التطبيق التشريعي حين يتوافر شرطان قانونيان متلازمان: الأول وجود نص تشريعي يُقرّر التزاماً قانونياً على جهة إدارية في مجال الأمن السيبراني، والثاني عجز هذه الجهة الموضوعي عن الوفاء بهذا الالتزام بسبب الفجوة الرقمية في مستوياتها الثلاثة المتقدم ذكرها. وحين يتوافر الشرطان معاً يُنتج ما يُمكن تسميته "التشريع المعلق" أي ذلك التشريع الذي يبقى معلقاً بين عالمين، عالم النص حيث يبدو فاعلاً وملزماً، وعالم التطبيق حيث يعجز عن إنتاج أثره القانوني المنشود^(٢٨). وما يُضفي على هذه الفجوة طابعاً قانونياً بالغ الخطورة هو أنها لا تتوقف عند حدود التقصير الإداري البسيط القابل للمعالجة بقرارات تنظيمية، بل تُنشئ ما يُسميه الفقه الإداري المقارن الالتزام المجوّف؛ وهو الالتزام القانوني الذي يحمل مضموناً نصياً كاملاً لكنه يفقد مضمونه الموضوعي بفعل العجز التطبيقي. والخطورة الفلسفية لهذا الالتزام المجوّف في سياق الضبط الإداري السيبراني تكمن في أنه يُضللّ المواطن بوهم الحماية ويُعطيه وصفاً قانونياً لحقوق لا يمتلك في الحقيقة القدرة على استيفائها^(٢٩).

ثانياً: تجليات فجوة التطبيق التشريعي في النظامين العراقي والمصري

تتجلى فجوة التطبيق التشريعي في التجربة العراقية بأجلى صورها وأوضح مظاهرها؛ فقانون التوقيع الإلكتروني والمعاملات الإلكترونية رقم ٧٨ لسنة ٢٠١٢ يشترط في المادة الأولى أن يكون التوقيع الإلكتروني "معتمداً من جهة التصديق"، وهو شرط يُعلن مشروعية قانونية مكتملة النص لكنه يصطدم بواقع مؤسسي لا تعمل فيه جهات التصديق الإلكتروني بالكفاءة المطلوبة، مما يجعل هذا الاشتراط التشريعي الجوهرى حبراً على ورق في كثير من حالات التطبيق^(٣٠). وعلى الصعيد الجنائي السيبراني، لا يزال العراق يفتقر إلى قانون متخصص للأمن السيبراني وإلى جهات ضبط إداري سيبراني واضحة الاختصاصات، مما يُفضي إلى أن كل تشريع ذي صلة يظل محاصراً في فجوة التطبيق ذاتها التي تحول دون إنتاجه لأثره القانوني المنشود^(٣١). أما في التجربة المصرية، فتتخذ فجوة التطبيق التشريعي شكلاً مغايراً يتعلق بالتفاوت في قدرة الجهات المختلفة على الامتثال للالتزامات التشريعية السيبرانية؛ فقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ يتضمن في المادة السابعة منه التزامات على مزودي الخدمة

بتطبيق معايير تقنية محددة لحماية البيانات، غير أن تطبيق هذه الالتزامات يتفاوت تفاوتاً ملحوظاً بين الجهات الحكومية الكبرى ذات الإمكانيات التقنية المتقدمة وبين الجهات الأصغر التي تعاني من محدودية الموارد التقنية والبشرية. وهذا التفاوت في التطبيق يُنتج ما يُمكن وصفه بالامتنال الانتقائي الذي يُطبّق النص على من يستطيع ويُعفي من لا يستطيع، وهو نوع من الامتنال يُقوّض مبدأ عموم القاعدة القانونية ويُفرغ التشريع من طابعه الإلزامي المطلق^(٣٢).

ثالثاً: الإشكالية القانونية لمساءلة الإدارة في ضوء فجوة التطبيق

تُثير فجوة التطبيق التشريعي إشكالية قانونية بالغة الدقة تتعلق بمدى إمكانية مساءلة الإدارة عن إخلالها بالتزاماتها السبيريانية حين تكون هذه الإخلال ناجمةً عن فجوة رقمية لا عن إهمال إرادي. فمن جهة، يقتضي مبدأ المسؤولية الإدارية أن تُساعِل الإدارة عن التقصير في أداء وظيفتها الضبطية، بصرف النظر عن الأسباب التي أفضت إلى هذا التقصير. ومن جهة أخرى، يقتضي مبدأ العدالة ومبدأ التناسب ألا تُحمّل الإدارة مسؤوليةً عن التقصير في أداء التزامات تتجاوز قدرتها الموضوعية الفعلية^(٣٣). والمخرج الفقهي الأسلم من هذه الإشكالية يكمن في التمييز بين مستويين من المسؤولية؛ المستوى الأول مسؤولية الإدارة عن التقصير في التطبيق ضمن حدود قدرتها القائمة، وهي مسؤولية لازمة لا تسقط بحجة الفجوة الرقمية. والمستوى الثاني مسؤولية الدولة عن الإخلال بالتزامها الأشمل ببناء القدرات اللازمة لتطبيق تشريعاتها، وهي مسؤولية سياسية وقانونية تقع على صانع القرار التشريعي والإداري لا على الموظف المنفّذ. وهذا التمييز بين مستويي المسؤولية يُتيح تأطيراً قانونياً متوازناً يحفظ مبدأ المساءلة دون أن يُفضي إلى مساءلة تعجيزية لإدارة تعمل في حدود ما أُتيح لها^(٣٤).

رابعاً: نحو معالجة قانونية لفجوة التطبيق التشريعي

لا يمكن معالجة فجوة التطبيق التشريعي بمجرد تشديد العقوبات على الجهات الإدارية المخلة أو تكثيف الرقابة عليها؛ فهذه الأساليب تُعالج الأثر دون أن تمسّ السبب. والمعالجة الحقيقية تستلزم مقارنة تشريعية مزدوجة تجمع بين مبدئين، مبدأ التشريع التدريجي الذي يربط الالتزامات القانونية السبيريانية بمستوى القدرات المؤسسية ويُدرجها تدريجياً كلما تحسّنت هذه القدرات، ومبدأ الالتزام بالبناء الذي يُقرّر مسؤولية قانونية صريحة على الدولة في بناء القدرات التقنية والبشرية اللازمة للوفاء بتشريعاتها السبيريانية ضمن جدول زمني ملزم. وهذان المبدآن يُحوّلان فجوة التطبيق من شُحٍّ في التنفيذ إلى أجندة إصلاحية واضحة المعالم قابلة للقياس والمساءلة^(٣٥).

المبحث الثاني

آليات معالجة الفجوة الرقمية وتعزيز مشروعية الضبط الإداري السيبراني

لا تقف هذه الدراسة عند حدود تشخيص الأزمة بل تتجاوزها إلى استشراف المسالك الإصلاحية الكفيلة بمعالجة الفجوة الرقمية وتعزيز مشروعية الضبط الإداري السيبراني. والمعالجة المنشودة ليست أحادية البعد تكتفي بالإصلاح التشريعي أو الاستثمار التقني أو إعادة الهيكلة المؤسسية كل على حدة، بل هي معالجة متكاملة تُعالج الأبعاد الثلاثة في استراتيجية واحدة منسجمة. وهذا ما يتناوله هذا المبحث في مطلبين؛ الأول للمستلزمات التشريعية والثاني للمستلزمات المؤسسية.

المطلب الأول

المستلزمات التشريعية لمعالجة الفجوة الرقمية

يحمل التشريع في منظومة الضبط الإداري السيبراني وظيفة مزدوجة لا يمكن اختزالها في أي من وجهيها دون الآخر؛ فهو من جهة أداة الإلزام التي تُحوّل الأهداف السياسية إلى واجبات قانونية قابلة للتطبيق والمساءلة، ومن جهة أخرى أداة التوجيه التي تُرسي القيم والمبادئ التي يسير في ضوئها الجهاز الإداري في مواجهة التهديدات السيبرانية. وغياب أي من الوجهين يُنتج تشريعاً منقوصاً؛ فالتشريع الذي يُلزم دون توجيه يُفضي إلى امتثال أعمى يفتقر إلى الفهم، والتشريع الذي يُوجه دون إلزام يُنتج توصيات بلا أسنان. وحين تُقرأ التشريعات السيبرانية القائمة في مصر والعراق في ضوء هذه الثنائية، يتكشف قصور مشترك في كليهما وإن اختلف شكله؛ ففي العراق يغيب التشريع الموحد فتضيع الوظائف معاً، وفي مصر يحضر التشريع لكنه يعاني من تشتت يُضعف وظيفة التوجيه ويُجزئ وظيفة الإلزام بين قوانين متعددة لا تتسق فيما بينها. وفي كلتا الحالتين تبقى فجوة التطبيق التشريعي قائمة وتظل المشروعية الغائبة للضبط الإداري السيبراني منقوصة. ولهذا لا تستقيم معالجة الفجوة الرقمية من زاويتها التشريعية بمجرد سدّ الثغرات النصية وتحديث القوانين المتقادمة، بل تستلزم بناء منظومة تشريعية متكاملة الطبقات تُجيب عن أربعة أسئلة جوهرية: ما الذي يُشرّع؟ وكيف يُنفذ؟ ومن يُساءل عند الإخلال؟ وكيف يُحدث دون أن يتحجّر؟ وقد جاء تقسيم هذا المطلب على فرعين يتناول الأول القانون الموحد للأمن السيبراني وحماية البيانات، ويتناول الثاني تحديث قوانين التوقيع الإلكتروني وترسيخ الرقابة القضائية.

الفرع الأول

القانون الموحد للأمن السيبراني وحماية البيانات

يُمثّل غياب القانون الموحد للأمن السيبراني في العراق وتشتت التشريعات السيبرانية في مصر الثغرة التشريعية الأكثر أثراً في إنتاج فجوة التطبيق وتوسيعها؛ فالقانون الموحد ليس مجرد وعاء

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجاً

تنظيمي يجمع نصوصاً متفرقة تحت مظلة واحدة، بل هو في فلسفته الأعمق إعلاناً للدولة عن رؤيتها المتكاملة لمسؤوليتها السيبرانية وتحديداً لمنهجها في تحقيق التوازن بين متطلبات الأمن وضمانات الحرية. فغياب هذا الإعلان يُبقي الضبط الإداري السيبراني سابقاً في فراغ مرجعي يجعل كل جهة تُفسّر مهامها وصلاحياتها وفق منطقها الداخلي لا وفق رؤية وطنية موحدة.

أولاً: مواصفات القانون الموحد للأمن السيبراني

لا تكفي الإحالة إلى نماذج مقارنة ناجحة لتحديد مواصفات القانون الموحد المنشود للعراق ومصر؛ فالقانون الجيد هو الذي يُصاغ استجابةً للسياق الخاص لا استنساخاً للنموذج الأجنبي. غير أن الدراسة المقارنة تكشف عن جملة من المواصفات الجوهرية التي ينبغي أن يستوفيه أي قانون موحد فاعل للأمن السيبراني بصرف النظر عن السياق. أولى هذه المواصفات هي الشمولية الثلاثية الأبعاد؛ إذ ينبغي أن يُعالج القانون الموحد الأمن السيبراني من ثلاث زوايا: الزاوية الجنائية التي تُجرّم الاعتداءات السيبرانية وتُحدد عقوباتها، والزاوية الإدارية الوقائية التي تُلزم الجهات الحكومية بمعايير حماية محددة وتُوزّع الاختصاصات وتُقرّر المسؤولية، والزاوية المدنية التي تُحدد التعويض المستحق للمتضررين من الاختراقات السيبرانية. وغياب أي من هذه الزوايا يُولّد فجوةً في المنظومة التشريعية يستغلها المعتدون السيبرانيون أو يُقيّد قدرة المتضررين على الانتصاف^(٣٦).

وثانيتهما الوضوح في توزيع الاختصاصات؛ إذ يُعدّ تشتت الاختصاص السيبراني بين جهات متعددة دون تحديد تشريعي دقيق من أبرز مسببات فجوة التطبيق. فالقانون الموحد ينبغي أن يُحدد بصورة قاطعة الجهة المرجعية العليا في منظومة الضبط الإداري السيبراني وصلاحياتها، والجهات التنفيذية وعلاقتها بالجهة المرجعية، وآليات الفصل في تنازع الاختصاص حين يقع. وهذا التوزيع الدقيق هو الشرط الضروري لتفعيل مبدأ المساءلة الإدارية؛ فلا مساءلة حقيقية حيث يسود الغموض في الاختصاص^(٣٧).

وثالثتها المرونة الدينامية؛ وهي الخاصية التي تُميّز التشريع السيبراني الناجح عن نظيره المتحجر؛ فالتهديدات السيبرانية تتجدد بوتيرة تفوق قدرة الدورة التشريعية التقليدية على مواكبتها. ولهذا ينبغي أن يُؤسّس القانون الموحد لآليةٍ لائحيةٍ مرنة تُتيح تحديث المعايير التقنية والإجراءات التشغيلية دون الحاجة إلى تعديل تشريعي في كل مرة تستجد فيها تقنية أو يبتكر المهاجمون أسلوباً جديداً. وهذا ما يُجسّده نموذج توجيه NIS2 الأوروبي الذي يُرسي المبادئ الجوهرية تشريعياً ويُفوّض اللوائح بالتفاصيل التقنية^(٣٨).

ثانياً: حماية البيانات الشخصية الحكومية مكوّناً ضرورياً للقانون الموحد

لا يكتمل القانون الموحد للأمن السيبراني دون أن يتضمن أو يرتبط ارتباطاً عضوياً بمنظومة حماية البيانات الشخصية الحكومية؛ فالبيانات التي تجمعها الجهات الحكومية عن مواطنيها تُمثّل ثروة معلوماتية واجبة الحماية بموجب مبدأ الأمانة الإدارية الذي يُلزم الإدارة بصون ما استؤمّنت عليه. وحين تُخترق هذه البيانات بسبب الفجوة الرقمية لا يكون الضرر لاحقاً بالمواطن وحده بل يكون الجهاز الإداري ذاته قد أخلّ بالأمانة الممنوحة إياه^(٣٩). وقد أحرزت مصر تقدماً ملموساً في هذا الشأن بإصدار قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ الذي أنشأ إطاراً لحوكمة البيانات يُلزم الجهات العامة بمعايير محددة في جمعها ومعالجتها وتخزينها، ومنح الأفراد جملةً من الحقوق الجوهرية أبرزها حق الحذف وحق الاعتراض على المعالجة وحق تصحيح البيانات الخاطئة^(٤٠). في المقابل، يفنقر العراق إلى تشريع مُوازٍ يُلزم الجهات الحكومية بمعايير محددة لحفظ بيانات المواطنين وتأمينها، وهو غياب يُؤلّد تناقضاً فلسفياً عميقاً في صميم العقد الاجتماعي الرقمي؛ فالدولة تطلب من مواطنيها تسليم بياناتهم الشخصية عبر المنصات الرقمية ولا تُقرّ في المقابل نصاً صريحاً يُحاسبها حين تُخفق في حمايتها^(٤١).

والدرس الأهم الذي تستخلصه هذه الدراسة من التجربة المصرية في هذا الشأن ليس الاحتذاء بالنموذج بل تجنب ثغراته؛ فقانون حماية البيانات المصري رقم ١٥١ لسنة ٢٠٢٠ صدر دون لوائح تنفيذية كاملة مما أوجد فجوة تطبيقية في المرحلة الأولى من تطبيقه. وهذه التجربة تُلقّن المشرّع العراقي المقبل على إصدار تشريع مشابه درساً بالغ الأهمية: إصدار اللائحة التنفيذية مع القانون لا بعده حتى لا يقع في الفجوة ذاتها التي حاول الفرار منها^(٤٢).

ثالثاً: نحو نموذج تشريعي مقترح للعراق

استناداً إلى ما تقدم، يمكن تحديد معالم النموذج التشريعي المقترح للعراق في ثلاثة محاور جوهرية: المحور الأول إصدار قانون موحد للأمن السيبراني يُعالج الأمن السيبراني من زوايا جنائية وإدارية ومدنية في وقت واحد مع إصدار لائحته التنفيذية التفصيلية معه لا بعده. والمحور الثاني ربط هذا القانون بمنظومة حماية البيانات الشخصية في إطار تشريعي متنسق يجمع بين الحماية الأمنية والحماية القانونية للبيانات. والمحور الثالث تضمين القانون آليةً لائحيةً مرنة تُتيح تحديث المعايير التقنية دون الحاجة إلى إعادة فتح باب التشريع في كل مرة تستجد فيها تقنية أو تهديد جديد^(٤٣).

الفرع الثاني

تحديث قانون التوقيع الإلكتروني وترسيخ الرقابة القضائية

يتناول هذا الفرع مستلزمين تشريعيين يبدوان للوهلة الأولى متباعين في موضوعهما؛ الأول تقني يتعلق بتحديث قوانين التوقيع الإلكتروني، والثاني قانوني دستوري يتعلق بترسيخ الرقابة القضائية على الضبط الإداري السيبراني. غير أن ما يجمعهما في فرع واحد ليس مجرد الاقتصاد في الترتيب بل وحدة فلسفية عميقة؛ فكلاهما يُعالج وجهاً من وجوه إشكالية واحدة هي مشروعية الضبط الإداري السيبراني من منظور مختلف: الأول يُعالجها من منظور الثقة في أدوات الضبط، والثاني يُعالجها من منظور الرقابة على ممارستها. ولا تكتمل المشروعية دون تكاملهما.

أولاً: تحديث قوانين التوقيع الإلكتروني في ضوء التطورات التقنية المستجدة

صيغ قانون التوقيع الإلكتروني المصري رقم ١٥ لسنة ٢٠٠٤ والقانون العراقي رقم ٧٨ لسنة ٢٠١٢ صيغا في حقبة لم تكن فيها تقنيات كالذكاء الاصطناعي والتوقيع البيومتري والبلوكشين قد بلغت مرحلة النضج التطبيقي التي بلغتها اليوم. والقانون الذي يُهمل استيعاب هذه التطورات يُعرض منظومة الضبط الإداري لفجوة تقنية تشريعية تستغلها تهديدات الغد بأدوات اليوم^(٤٤). وتتجلى الحاجة إلى التحديث في ثلاثة محاور رئيسية؛ أولها استيعاب التوقيع البيومتري وتحديد شروط الاعتراد به قانونياً بوصفه بديلاً أو مكماً للتوقيع الرقمي التقليدي، مع تحديد الضمانات اللازمة لمنع التزوير البيومتري الذي بات ممكناً بتقنيات التزييف العميق (Deep Fake). وثانيها وضع إطار قانوني لتوثيق المعاملات الإدارية على تقنية البلوكشين التي تُتيح إنشاء سجلات رقمية غير قابلة للتعديل تحافظ على سلامة المستندات الحكومية بصورة تفوق ما يُوفره التفسير التقليدي. وثالثها تنظيم استخدام الذكاء الاصطناعي في عمليات التحقق من الهوية وإعطائها حجية قانونية مكافئة للتحقق البشري المتعارف عليه قانوناً وفق شروط ضمانية محددة^(٤٥).

وفي سياق التجربة المقارنة، يستلفت الانتباه أن توجيه eIDAS الأوروبي ونظيره المحدث eIDAS2 قد اعتمدا نهجاً تشريعياً مرناً يُرسي المبادئ الجوهرية للتوقيع الإلكتروني تشريعياً ويُفوض اللوائح التقنية بالتفاصيل القابلة للتحديث المستمر. وهذا النهج يُمثل الدرس الأبلغ لكل من المشرعين المصري والعراقي؛ إذ إن قانون التوقيع الإلكتروني الجيد ليس القانون الذي يُحدد التقنية بل القانون الذي يُرسي المبادئ التي تحكم أي تقنية قادمة^(٤٦). ولا يقتصر التحديث على النصوص التشريعية بل يمتد ليشمل جهات التصديق الإلكتروني ذاتها؛ فهذه الجهات هي الذراع المؤسسية التي تُحوّل الحجية القانونية للتوقيع إلى واقع تقني قابل للتطبيق. وفي العراق حيث لا



تعمل جهات التصديق بالكفاءة المطلوبة، يبقى التوقيع الإلكتروني حقاً قانونياً بلا أداة تنفيذية فعّالة. ومن هنا يُصبح تطوير جهات التصديق الإلكتروني وتقنياتها بمعايير واضحة شرطاً لازماً لأي تحديث تشريعي حقيقي، لأن القانون الجيد مع مؤسسة هشّة لا ينتج ضبطاً فاعلاً.^(٤٧)

ثانياً: ترسيخ الرقابة القضائية على الضبط الإداري السيبراني

يُمثل ترسيخ الرقابة القضائية على الضبط الإداري السيبراني المستلزم التشريعي الأعمق في هذه المنظومة الإصلاحية؛ فالضبط الإداري الذي لا تراقبه جهة قضائية مستقلة وكفوءة ينزلق حتماً نحو التوسع التعسفي الذي يُفضي إلى ما يُسميه الفقه الإداري الضبط المفرط الذي يُخلّ بالتوازن بين الأمن والحرية ويُقوّض المشروعية الغائية للضبط ذاته. وتُجسّد المادة ٢٥ من قانون ١٧٥ لسنة ٢٠١٨ المصري المتعلقة بالقيم الأسرية نموذجاً صريحاً لهذا الخطر؛ إذ أتاحت للجهات الإدارية هامشاً من التقدير الواسع انتقدته منظمات حقوق الإنسان لكونه قابلاً لتوظيف غير متناسب مع الغاية التشريعية المُعلنة^(٤٨). وتستلزم الرقابة القضائية الفاعلة على الضبط الإداري السيبراني ثلاثة شروط تشريعية متلازمة؛ أولها التخصص القضائي الذي يعني ضرورة إنشاء دوائر قضائية أو على الأقل تكوين قضاة متخصصين في المنازعات الإدارية الرقمية قادرين على تقدير الأبعاد التقنية للنزاع دون الاستسلام الكامل لرأي الخبير. فالقاضي الذي يجهل أبعاد الفضاء السيبراني لا يستطيع تقييم مشروعية تدابير الضبط الإداري السيبراني تقييماً حقيقياً ويتحول دوره من رقيب فاعل إلى مُصادق شكلي^(٤٩). وثانيها سرعة الفصل التي تُعدّ شرطاً وظيفياً لا ترفاً إجرائياً؛ فالتدابير السيبرانية ذات طابع استعجالي في الغالب، وأثرها يمتد ويتعمق مع مرور الوقت، مما يعني أن رقابة قضائية بطيئة تفقد جدواها في أغلب الأحيان. ولهذا ينبغي أن تُؤسّس التشريعات لإجراءات قضائية استعجالية خاصة بمنازعات الضبط الإداري السيبراني تنظر فيها المحاكم المختصة في مدد قصيرة.^(٥٠) وثالثها مبدأ التناسب الذي يُعدّ المعيار الأمثل لرقابة القضاء الإداري على تدابير الضبط السيبراني؛ فالقضاء ينظر في مدى تناسب التدبير الإداري مع حجم التهديد المُبرّر به ومع ما يُسببه من قيود على الحريات الرقمية. وقد أرست المحكمة الأوروبية لحقوق الإنسان أحكاماً لافتة في هذا الشأن اشترطت ثلاثة شروط تراكمية لمشروعية أي تدبير سيبراني مقيد للحريات: وجود نص قانوني صريح، وهدف مشروع، وتناسب صارم بين الإجراء والهدف^(٥١).

وفي تجربة مصر والعراق، تبقى الرقابة القضائية على تدابير الضبط الإداري السيبراني محدودةً نطاقاً وغير متخصصة. ففي مصر لا توجد دوائر قضائية متخصصة في المنازعات الإدارية الرقمية، وفي العراق يزيد من ضعف الرقابة غياب التشريع الموحد ذاته الذي يُوفر

المرجعية القانونية التي يُقيس عليها القاضي مشروعية التدابير. ومن هنا تتكشف الحلقة المفرغة الكاملة: غياب التشريع يُضعف الرقابة القضائية، وضعف الرقابة القضائية يُشجع على إهمال إصدار التشريع، والنتيجة ضبطٌ إداري سيبراني يعمل في فراغ من المشروعية يُنتج انكشافاً من جهة وتعسفاً من جهة أخرى^(٥٢).

المطلب الثاني

المستلزمات المؤسسية لتعزيز مشروعية الضبط الإداري السيبراني

ثمة حقيقة يُرسّخها تاريخ الإصلاح الإداري في دول كثيرة مفادها أن التشريع الجيد في غياب المؤسسة الفاعلة لا يُنتج إلا وعوداً مكتوبة؛ فالنص القانوني مهما بلغت جودته لا يلزم من تلقاء ذاته بل يحتاج إلى جهاز مؤسسي يُترجمه إلى ممارسة يومية ويرصد الامتثال به ويُحاسب على الإخلال بأحكامه. وفي مجال الضبط الإداري السيبراني تتضاعف هذه الحاجة المؤسسية؛ فالفضاء السيبراني بطبيعته الديناميكية المتجددة لا يحتمل الانتظار حتى تتحرك الدورة التشريعية لمعالجة كل تهديد مستجد، بل يستلزم مؤسسات ذات قدرة استجابة لحظية وكوادر بشرية متخصصة وآليات تنسيق تجعل من الجهاز الإداري كلاً متماسكاً لا أجزاءً متناثرة. وما يجعل البُعد المؤسسي في السياق المصري والعراقي ذا أولوية استثنائية هو أن كلا البلدين يعانيان من إشكالية التشتت المؤسسي التي أفرزت نمطاً من الضبط الإداري السيبراني المتقطع؛ نشاطاً هنا وثغرةً هناك، واختصاصٌ متنازع عليه في المنتصف. وهذا النمط لا يُعالج بإصدار قانون جديد بل بإعادة هيكلة مؤسسية شاملة تُرسي خريطة واضحة للاختصاصات وتوفر الأدوات البشرية والتنسيقية اللازمة لتفعيلها. وقد جاء تقسيم هذا المطلب على فرعين؛ يتناول الأول ضرورة وجود هيئة وطنية مستقلة، ويتناول الثاني التنسيق المؤسسي وشراكة القطاع الخاص.

الفرع الأول

هيئة وطنية مستقلة

يُجسّد هذا الفرع الوجه الأكثر ملموسيةً في منظومة المستلزمات المؤسسية؛ فبينما تبقى التشريعات في عالم المجرّد القانوني حتى يُجسّدّها جهازٌ مؤسسي فاعل، تُحوّل الهيئة الوطنية والكادر البشري المتخصص الضبط الإداري السيبراني من مفهوم قانوني نظري إلى ممارسة إدارية يومية. وما يُضفي على هذين العنصرين أهميةً استثنائيةً في سياق هذه الدراسة هو أنهما يُعالجان في آنٍ واحد وجهين متكاملين من وجوه فجوة الاستمرارية؛ فالهيئة توفر الاستمرارية المؤسسية، والكادر البشري يوفر الاستمرارية الوظيفية، وبدون تكاملهما يظل الضبط الإداري السيبراني رهين الظروف لا سيداً عليها.

أولاً: الهيئة الوطنية المستقلة للأمن السيبراني

يُعدّ إنشاء هيئة وطنية مستقلة للأمن السيبراني ذات صلاحيات تنظيمية وإشرافية واضحة من أكثر المستلزمات المؤسسية إلحاحاً وأوضحها أثراً في سدّ فجوة التشتت المؤسسي. فالتجارب الدولية الناجحة تكشف دون استثناء تقريباً أن الدول التي أحرزت تقدماً ملموساً في منظومة ضبطها الإداري السيبراني هي تلك التي أسست مرجعيةً مؤسسيةً موحّدة تضطلع بمهمة التنسيق والإشراف والمساءلة^(٥٣).

وتمثّل وكالة ANSSI الفرنسية النموذج الأكثر نضجاً في هذا الشأن؛ فهي هيئة تتبع رئيس الوزراء وتتمتع بصلاحيات خمس متكاملة: الدفاع عن الأنظمة الحيوية، ورصد التهديدات، وتبادل الخبرات والتوصيات، ومراقبة المؤسسات في تطبيق معايير الأمن، وتنظيم المنتجات والخدمات السيبرانية. وما يُميّز ANSSI عن كثير من الهيئات المماثلة هو استقلاليتها الكافية عن الأجهزة الأمنية التنفيذية مما يجعلها جهةً تنظيميةً لا أداةً استخباراتية، وهو تمييز ذو أهمية دستورية بالغة في ضمان أن لا يُحوّل الضبط الإداري السيبراني إلى أداة قمع رقمي^(٥٤).

وفي ضوء هذا النموذج يتبيّن أن مصر أحرزت تقدماً ملموساً بإنشاء المجلس الأعلى للأمن السيبراني والمركز المصري للاستجابة للطوارئ المعلوماتية (EG-CERT)، غير أن هذا الإنجاز يعاني من قصور في وحدة المرجعية وتكامل الصلاحيات؛ فالمجلس الأعلى هيئة استشارية تنسيقية لا هيئة تنفيذية ذات صلاحيات ملزمة، مما يُضعف قدرتها على فرض معايير الأمن السيبراني على الجهات الحكومية المتفاوتة في مستويات امتثالها^(٥٥). أما في العراق فيفتقر الجهاز الإداري إلى مؤسسة مرجعية سيبرانية موحّدة، وتتوزع المهام بين أجهزة أمنية ووزارية متعددة دون خريطة اختصاصات واضحة، مما يُولّد فراغاً مؤسسياً يستغله كل من يبحث عن ثغرة في منظومة الضبط^(٥٦).

وينبغي أن تتمتع الهيئة الوطنية المقترحة بخمسة مقومات جوهرية تُكسبها فاعليتها: الاستقلالية عن الأجهزة الأمنية التنفيذية لضمان حياديتها التنظيمية، والصلاحيات الملزمة لإصدار معايير أمنية على الجهات الحكومية ومتابعة تطبيقها، وآلية مساءلة واضحة تُحدد المسؤولية عند الإخلال بهذه المعايير، والتمثيل المتوازن بين الجهات الحكومية والقطاع الخاص والمجتمع المدني في هياكلها الحوكمية، وأخيراً ربطها بشبكة التعاون الدولي والإقليمي في مجال الأمن السيبراني لضمان تبادل المعلومات الاستخباراتية السيبرانية في الوقت الفعلي^(٥٧).

ثانياً: بناء الكوادر البشرية المتخصصة

يُشكّل الكادر البشري المتخصص في الأمن السيبراني الأصل الاستراتيجي الأثمن في منظومة الضبط الإداري السيبراني؛ فالهيئة الوطنية مهما بلغت متانة هيكلها القانوني وسعة صلاحياتها تظل أداة بلا أسنان إن لم تُحرّكها كوادر بشرية تمتلك الكفاءة الفنية والوعي القانوني والحس المؤسسي اللازم للتصدي للتهديدات السيبرانية. وهذه الحقيقة يؤكدّها الواقع الإحصائي بصورة صريحة؛ إذ أثبتت الدراسات الميدانية أن نسبة كبيرة من الاختراقات السيبرانية للأجهزة الحكومية تبدأ من ثغرات بشرية لا تقنية، مما يعني أن الاستثمار في التدريب والتنشئة المهنية للكوادر الإدارية لا يقل أهمية عن الاستثمار في الأجهزة والبرمجيات^(٥٨).

وتتكشف من المقارنة بين التجريبتين المصرية والعراقية فجوة بشرية واسعة لا تقل خطورة عن الفجوة التشريعية والمؤسسية؛ فعلى الرغم من الجهود المصرية في تطوير برامج تدريب الكوادر الحكومية على الأمن السيبراني، تبقى الهوة واسعة بين العدد الفعلي للمتخصصين السيبرانيين في الجهاز الإداري وبين الحاجة الفعلية لهم. أما في العراق، فيزيد الأمر تعقيداً عجز الإدارة عن المنافسة مع القطاع الخاص والشركات الأجنبية في استقطاب الكفاءات الشابة المتخصصة في أمن المعلومات، مما يُنتج ما يُسميه الفقه الإداري المقارن "نزيف الكفاءات السيبرانية" الذي يُجفّف منابع الضبط الإداري من داخله^(٥٩).

وتستلزم معالجة هذه الفجوة البشرية استراتيجية وطنية متكاملة تقوم على ثلاثة محاور متوازية؛ أولها التأهيل الأكاديمي الذي يعني تطوير مناهج متخصصة في القانون الرقمي والأمن السيبراني في الجامعات، وإنشاء برامج دراسات عليا متخصصة تجمع بين التكوين القانوني الإداري والكفاءة التقنية السيبرانية. وثانيها التدريب المستمر الذي يعني إلزام موظفي الأجهزة الحكومية بدورات تدريبية دورية في الأمن السيبراني وفق مستويات متدرجة تناسب طبيعة عمل كل موظف؛ فالوعي الأمني المطلوب من مدير قاعدة البيانات يختلف عن الوعي المطلوب من موظف الاستقبال، لكن كليهما ضروري في منظومة الدفاع السيبراني المؤسسي^(٦٠). وثالثها الاستبقاء المؤسسي الذي يعني إيجاد حوافز تنافسية تُغري الكفاءات السيبرانية بالعمل في الجهاز الحكومي بدلاً من هجرته نحو القطاع الخاص؛ فالمعركة على الكفاءات السيبرانية ليست حرباً حكومية داخلية بل هي حرب بين الحكومة والقطاع الخاص والدول الأجنبية، ولا يمكن للجهاز الإداري الفوز بها بأدوات الخدمة المدنية التقليدية وحدها.

وخلاصة ما يُخلص إليه أن الهيئة الوطنية المستقلة والكادر البشري المتخصص ليسا خيارين مؤسسيين يُختار بينهما بل ضرورتان متلازمتان تُكمل كل منهما الأخرى؛ هيئة بلا كادر هيكلٌ

بلا روح، وكادراً بلا هيئة طاقة بلا توجيه. وهذا التكامل هو الشرط الأساسي لتحويل الضبط الإداري السيبراني من مفهوم قانوني نظري إلى منظومة حوكمة رقمية فاعلة وقادرة على مواجهة تحديات الفضاء السيبراني بوعي وكفاءة واستدامة.

الفرع الثاني

التنسيق المؤسسي ومشاركة القطاع الخاص

يُعالج هذا الفرع البُعد التكاملي في منظومة الضبط الإداري السيبراني؛ فحين تُؤسس الهيئة الوطنية وتُبنى الكوادر البشرية يبقى السؤال الأعمق: كيف تعمل هذه العناصر معاً في منظومة متسقة؟ وكيف يمتد الضبط الإداري السيبراني إلى ما هو خارج حدود الجهاز الحكومي نحو القطاع الخاص الذي يسيطر على جزء كبير من البنية التحتية الرقمية؟ للإجابة على هذه التساؤلات نتبع الاتي:

أولاً: التنسيق المؤسسي بين الجهات المعنية بالضبط الإداري السيبراني

يُعدّ غياب التنسيق المؤسسي بين الجهات المعنية بالأمن السيبراني من أبرز الأسباب البنوية التي تُفضي إلى فجوة التطبيق التشريعي التي تناولناها في المطلب الأول؛ فحين تتعدد الجهات التي تدّعي الاختصاص السيبراني دون آلية تنسيق فاعلة تنشأ حالة من التداخل في الصلاحيات والفراغ في المسؤولية في آنٍ واحد، مما يُفضي إلى جهود متوازية لا تتكامل وتهديدات تنفلت من الشقوق التي تُحدثها حدود الاختصاص المتنازع عليه^(٦١). وتتجلى هذه الإشكالية في التجربة العراقية بصورة حادة؛ إذ تتوزع المهام السيبرانية بين وزارة الداخلية وجهاز الأمن الوطني وهيئة الاتصالات والإعلام ووزارة الدفاع دون مرجعية تنسيقية موحدة، مما يُنتج ما يمكن تسميته بالضبط المتعدد الرؤوس الذي يبدو قوياً في شكله لكنه يفتقر إلى الفاعلية لغياب الإرادة الموحدة. وعلى الرغم من أن مصر قطعت شوطاً أبعد في هذا الاتجاه من خلال المجلس الأعلى للأمن السيبراني، تبقى إشكالية التنسيق حاضرة في العلاقة بين المجلس وهيئة ITIDA والجهاز القومي لتنظيم الاتصالات وسائر الجهات ذات الصلة^(٦٢).

والتنسيق المؤسسي الفاعل يستلزم أربعة عناصر متكاملة؛ أولها مرجعية واحدة للقرار تُحدد جهةً بعينها تملك القرار النهائي في الحالات التي تتداخل فيها الاختصاصات. وثانيها بروتوكولات تشغيلية موحدة تُحدد آليات التعامل مع الحوادث السيبرانية وتوزيع الأدوار بين الجهات المختلفة في كل مرحلة من مراحل الاستجابة. وثالثها منصة مشتركة لتبادل المعلومات تُتيح للجهات المعنية تبادل بيانات التهديدات في الوقت الفعلي دون الحاجة إلى إجراءات بيروقراطية تُبطئ

الاستجابة. ورابعها آلية مساءلة مشتركة تُحدد مسؤولية كل جهة في الحوادث التي وقعت بسبب قصور في التنسيق وتُقرّر التبعات الإدارية المترتبة على ذلك^(٦٣).

وقد أثبت نموذج JCDC الأمريكي (Joint Cyber Defense Collaborative) الذي تناولته هذه الدراسة في موضع سابق أن التنسيق المؤسسي الفاعل لا يستلزم بالضرورة إلغاء الاختصاصات القائمة بل يستلزم بناء آلية تنسيق عليها تستوعب هذه الاختصاصات وتوجهها نحو هدف مشترك. فالدرس الأبلغ من هذا النموذج للتجربتين المصرية والعراقية هو أن التنسيق ليس عملية إدارية روتينية بل هو في جوهره قرار سياسي بوحدة الرؤية الوطنية في مواجهة التهديدات السيبرانية^(٦٤).

ثانياً: شراكة القطاع الخاص في منظومة الضبط الإداري السيبراني

يُمثل إشراك القطاع الخاص في منظومة الضبط الإداري السيبراني تحولاً فلسفياً عميقاً في مفهوم الدولة وعلاقتها بالفاعلين غير الحكوميين؛ فالنموذج الكلاسيكي للضبط الإداري يقوم على ثنائية واضحة: دولة تضبط وأفراد/مؤسسات تخضع للضبط. غير أن الفضاء السيبراني أفرز واقعاً جديداً يُعقّد هذه الثنائية ويُبطل منطقها؛ إذ إن ٨٥% من البنية التحتية الرقمية الحيوية في معظم الدول تُديرها شركات خاصة لا جهات حكومية، مما يعني أن الدولة لا تستطيع أن تضبط فضاءً تسيطر الشركات الخاصة على جزء جوهري من بنيته^(٦٥).

وهذه الحقيقة تدفع نحو إعادة تعريف العلاقة بين الدولة والقطاع الخاص في الفضاء السيبراني من علاقة المنظم والمنظم إلى علاقة الشركاء المتكاملين الذين تجمعهم مصلحة مشتركة في أمن الفضاء الرقمي وإن اختلفت دوافعهم وأولوياتهم. والدولة في هذا النموذج التشاركي الجديد لا تتخلى عن سلطاتها التنظيمية بل تُعيد توظيفها؛ من ضبط قائم على الأوامر والنواهي إلى ضبط قائم على الحوافز والمعايير والتنسيق الفاعل مع من تملك الشركات الخاصة من قدرات يفقر إليها الجهاز الحكومي^(٦٦).

وتتجلى أهمية هذه الشراكة في التجربتين المصرية والعراقية بصور متعددة؛ فمزودو خدمات الإنترنت والاتصالات يمتلكون بيانات حركة الشبكة اللازمة للكشف المبكر عن الهجمات السيبرانية، وشركات الحوسبة السحابية تستضيف بيانات حكومية حساسة وتملك أدوات الحماية اللازمة لها، وشركات الأمن المعلوماتي تتوفر لديها خبرات تقنية متقدمة تفوق في كثير من الأحيان ما يتوفر في الجهاز الحكومي. وكل هذه القدرات لا يمكن توظيفها في خدمة الضبط الإداري السيبراني دون إطار قانوني للشراكة يُحدد حقوق والتزامات كل طرف ويوازن بين متطلبات أمن الدولة ومتطلبات السرية التجارية^(٦٧). ولتأطير هذه الشراكة قانونياً وإدارياً تستلزم

الدراسة ثلاثة مقومات جوهرية؛ أولها إطار قانوني واضح يُحدد التزامات القطاع الخاص في الإبلاغ عن الحوادث السيبرانية وتطبيق معايير الأمن المحددة والتعاون مع جهات الضبط الإداري عند الطلب، دون أن يُفضي ذلك إلى فرض أعباء تنافسية غير متناسبة تُضرّ بالبيئة الاستثمارية. وثانيها آليات تبادل المعلومات بين الجهات الحكومية والقطاع الخاص في الوقت الفعلي، مع توفير الضمانات القانونية الكافية لحماية البيانات التجارية الحساسة التي يُفصح عنها القطاع الخاص في إطار هذا التبادل. وثالثها تحفيز الامتثال من خلال منح الشركات الملتزمة بمعايير الأمن السيبراني المحددة مزايا تفضيلية في عقود الحكومة وتكريمها في المؤشرات الوطنية للمسؤولية الرقمية؛ فالامتثال الطوعي المُحفّز أكثر فاعليّة واستدامةً من الامتثال القسري المفروض بعقوبات وحدها^(٦٨).

وفي الختام، يُمثّل التكامل بين التنسيق المؤسسي وشراكة القطاع الخاص الشرط الموضوعي لاكتمال المنظومة المؤسسية للضبط الإداري السيبراني؛ فالتنسيق بين الجهات الحكومية يُضمن وحدة الإرادة الوطنية في مواجهة التهديدات، والشراكة مع القطاع الخاص تُضمن شمولية الحماية ووصولها إلى كامل البنية التحتية الرقمية. وبدون هذا التكامل المزدوج يبقى الضبط الإداري السيبراني ناقص الأثر مهما تقدمت تشريعاته وتطورت هيئاته الرسمية.

الخاتمة

خلصت هذه الدراسة إلى جملة من النتائج والتوصيات يمكن إجمالها على النحو الآتي:

أولاً: النتائج

١- إن الفجوة الرقمية في سياق القانون الإداري ليست ظاهرةً تقنيةً أو اقتصاديةً بحتة، بل هي اختلالٌ هيكلي يمسّ مشروعية الضبط الإداري السيبراني من بُعديها، المشروعية الشكلية التي تتعلق بصحة الإجراءات، والمشروعية الغائية التي تتعلق بالقدرة الفعلية على تحقيق النظام العام الرقمي. وحين تعجز الإدارة عن الوفاء بوظيفتها الضبطية السيبرانية بسبب الفجوة الرقمية يتحقق خللٌ في المشروعية الغائية حتى وإن توافرت النصوص التشريعية الكافية، مما يجعل معالجة الفجوة الرقمية شرطاً قانونياً لازماً لا مجرد هدف تنموي مستحسن.

٢- إن الفجوة الرقمية تُخلّ بمبدأين راسخين في القانون الإداري المقارن؛ أولهما مبدأ استمرارية المرفق العام الذي لا يقتصر في مفهومه الحديث على منع الانقطاع الفعلي بل يمتد ليشمل واجب الإدارة في اتخاذ التدابير الوقائية اللازمة للحيلولة دون الانقطاع المحتمل، وثانيهما مبدأ المساواة أمام المرافق العامة الذي تنتهكه الفجوة الرقمية حين تُفضي إلى تفاوت في مستوى الحماية السيبرانية بين المناطق الجغرافية والجهات الإدارية المختلفة.

الفجوة الرقمية و أثرها على مشروعية الضبط الإداري السيبراني مصر والعراق أنموذجاً

٣- تتمايز التجربتان المصرية والعراقية في طبيعة الفجوة الرقمية التي تعانيان منها لا في مجرد حدتها؛ فمصر تعاني من فجوة الاتساق المؤسسي المتمثلة في التشتت التشريعي وضعف التنسيق بين الجهات المتعددة وتفاوت التطبيق بين القطاعات، في حين يعاني العراق من "الفجوة البنيوية الشاملة" التي تظال البنية التحتية والكوادر البشرية والإطار التشريعي والمؤسسي في آن واحد. وهذا التمايز في طبيعة الفجوة يستلزم استجاباتٍ إصلاحيةً مختلفة في مساراتها وإن تقاطعت في مبادئها.

٤- يكشف تحليل فجوة التطبيق التشريعي أن ثمة مسؤوليةً قانونيةً مزدوجة تترتب على الدولة في مواجهة الفجوة الرقمية؛ مسؤولية تنفيذية تقع على الجهاز الإداري في التطبيق ضمن حدود قدرته القائمة، ومسؤولية تأسيسية تقع على صانع القرار التشريعي والسياسي في بناء القدرات اللازمة للوفاء بالتشريعات السيبرانية ضمن جدول زمني ملزم.

٥- إن الإصلاح الفاعل لمنظومة الضبط الإداري السيبراني يستلزم تكاملاً بين مستويين لا يُغني أحدهما عن الآخر: مستوى تشريعي يُوفر الشرعية والإلزامية والمرونة الدينامية، ومستوى مؤسسي يُجسّد هذه الشرعية في هياكل وكوادر وآليات تحوّلها من نص مكتوب إلى ممارسة إدارية راسخة. وأي إصلاح يُعالج أحد المستويين دون الآخر يُنتج بناءً منقوصاً لا يصمد أمام التهديدات السيبرانية المتصاعدة.

ثانياً: التوصيات

١ - الدعوة إلى إصدار قانون موحد للأمن السيبراني في العراق يُعالج مسألة التنظيم من ثلاث زوايا متكاملة في وقت واحد؛ الزاوية الجنائية التي تُجرّم الاعتداءات السيبرانية وتُحدد عقوباتها، والزاوية الإدارية الوقائية التي تُلزم الجهات الحكومية بمعايير حماية محددة وتُوزّع الاختصاصات وتُقرّر المسؤولية عند الإخلال، والزاوية المدنية التي تُحدد التعويض المستحق للمتضررين من الاختراقات السيبرانية. ويستلزم هذا القانون إصدار لائحته التنفيذية التفصيلية في ذات الوقت لا بعده، تجنباً لفجوة التطبيق التي كشف عنها هذا البحث وأثبتت التجربة المقارنة خطورتها.

٢ - الدعوة إلى إنشاء هيئة وطنية مستقلة للأمن السيبراني في العراق تتمتع بصلاحيات تنظيمية وإشرافية وتنسيقية واضحة، تكون مرجعيةً موحدة تُنهي التشتت المؤسسي الذي كشف عنه البحث وتُوحّد جهود الضبط الإداري السيبراني نحو رؤية وطنية متكاملة. ويُشترط في هذه الهيئة أن تتمتع باستقلالية كافية عن الأجهزة الأمنية التنفيذية حتى لا يُحوّل الضبط الإداري السيبراني أداةً للقمع الرقمي بدلاً من الحماية السيبرانية.



٣ - الدعوة إلى تطوير الرقابة القضائية على الضبط الإداري السيبراني، وذلك من خلال تأهيل القضاء الإداري للنظر في المنازعات الرقمية بما يستلزمه ذلك من تكوين قانوني تقني متخصص، وإرساء إجراءات قضائية استعجالية خاصة بهذا النوع من المنازعات، وترسيخ مبدأ التناسب بوصفه المعيار الأمثل لرقابة مشروعية التدابير السيبرانية في مواجهة الحريات الرقمية. وتتبقى أهمية هذا المقترح من الحقيقة التي أرساها هذا البحث وهي أن الضبط الإداري السيبراني الذي لا تراقبه جهة قضائية مستقلة وكفوءة ينزلق حتماً نحو التوسع التعسفي الذي يقوّض مشروعيته الغائية.

الهوامش

(١) د. زانا جلال سعيد، الموازنة بين الضبط الإداري والحريات العامة والرقابة القضائية عليها، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٧، ص ٣٠.

(٢) التحول الرقمي في الإدارة العامة وتحدياته القانونية، دراسة متعددة الأبعاد للفترة ٢٠١٠-٢٠٢٤، متاح على: <https://archives.univ-eloued.dz/items/16af273b-fa79-49c4-93c1-050f2d8deda9>

(٣) المصدر نفسه.

(٤) (International Telecommunication Union (ITU), Global Cybersecurity Index Report 2023, Geneva, pp.49-51.

(٥) مصباح أبوبكر مصباح، دور الموظفين في تعزيز أو إضعاف أمن المعلومات بالمؤسسات، مجلة جامعة فزان العلمية، المجلد ٤، العدد ٢، يونيو ٢٠٢٥، ص ١٣٥.

(٦) محمد كاظم هادي عنجور المنصوري، الواقع التشريعي للأمن السيبراني في العراق: التحديات والطموحات، مجلة العلوم الإنسانية والطبيعية (HNSJ)، المجلد ٦، العدد ٨، أغسطس ٢٠٢٥، ص ٥٦١.

(٧) بلعوسي أمين وعبابسة حمزة، أثر الأمن السيبراني والضبط الإداري على الحقوق والحريات في العصر الرقمي، مجلة القانون والمجتمع والسلطة، العدد ١٤، ٢٠٢٥، ص ١٩٩.

(٨) د. حسين أحمد مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة ٦٥، يناير ٢٠٢٣، ص ٦٧١.

(٩) رنا ياسين حسين، الضبط الإداري الإلكتروني في مواجهة الحريات الرقمية، مجلة العصر للعلوم الإنسانية والاجتماع، المجلد ٢٢، أبريل ٢٠٢٦، ص ٢٠٨.

(١٠) هيئة الاستعلامات المصرية، مصر ضمن أفضل ١٢ دولة أداءً بمؤشر الأمن السيبراني العالمي ٢٠٢٤، متاح على: <https://www.sis.gov.eg/Story/308803>

(١١) المصدر نفسه.

(١٢) تكشف مصر عن رقم فلكي في عدد الهجمات الإلكترونية التي تعرضت لها في ٢٠٢٤.

(١٣) مصطفى كامل الشريف، السيادة الرقمية الغائبة وسقوط حر في المؤشرات الدولية، ٢٠٢٤، متاح على: <https://itach.dk/egdi-gci>.

- (^{١٤}) المصدر نفسه.
- (^{١٥}) محمد كاظم هادي عنجور المنصوري، مصدر سابق، ص ٥٦٨.
- (^{١٦}) مصطفى كامل الشريف، نموذج تحليل الدولة الرقمية: من الاتصال إلى السيادة الرقمية، مصدر سابق.
- (^{١٧}) المصدر نفسه.
- (^{١٨}) سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني، مجلة جامعة واسط، مجلد ٣، ٢٠٢٢، ص ٥٣٢.
- (^{١٩}) (Mostafa Ali Elokaby, Development of cybersecurity laws in Egypt and its impact on the judicial system, International Cybersecurity Law Review, Vol. 5, No. 4, October 2024, p.580.
- (^{٢٠}) د. ياسر محمد عبد السلام رجب، دور الضبط الإداري في الرقابة السيبرانية وتهيئة البيئة السيبرانية الأمانة، مجلة القانون والتكنولوجيا، المجلد ١، العدد ١، أبريل ٢٠٢٢، ص ١٤٩.
- (^{٢١}) د. حسين أحمد مقداد عبد اللطيف، مصدر سابق، ص ٦٧١.
- (^{٢٢}) سامر محي عبد الحمزة، مصدر سابق، ص ٥٣٢.
- (^{٢٣}) بلعروسي أمين وعبابسة حمزة، مصدر سابق، ص ١٩٩.
- (^{٢٤}) زانا جلال سعيد، الموازنة مصدر سابق، ص ٣٠.
- (^{٢٥}) مصطفى كامل الشريف، السيادة الرقمية الغائبة وسقوط حر في المؤشرات الدولية، ٢٠٢٤ مصدر سابق
- (^{٢٦}) (Mostafa Ali Elokaby, op.cit, p.575.
- (^{٢٧}) رنا ياسين حسين، مصدر سابق، ص ٢٠٨.
- (^{٢٨}) د. حسين أحمد مقداد عبد اللطيف، مصدر سابق، ص ٦٩٢.
- (^{٢٩}) رنا ياسين حسين، مصدر سابق، ص ٢٠٨.
- (^{٣٠}) قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢، المادة الأولى؛ وينظر: فاضل علي حسوني، التوقيع الإلكتروني وحجيته في الإثبات، مجلة رسالة الحقوق، المجلد ٨، العدد ١، ٢٠١٦، ص ٤٢٢.
- (^{٣١}) محمد كاظم هادي عنجور المنصوري، مصدر سابق، ص ٥٦١.
- (^{٣٢}) (Mostafa Ali Elokaby, op.cit, p.575.
- (^{٣٣}) بلعروسي أمين وعبابسة حمزة، مصدر سابق، ص ٢٠٠.
- (^{٣٤}) د. زانا جلال سعيد، الموازنة بين الضبط الإداري والحريات العامة والرقابة القضائية عليها، مصدر سابق، ص ٣٥.
- (^{٣٥}) مصطفى كامل الشريف، نموذج تحليل الدولة الرقمية، ٢٠٢٦، مصدر سابق.
- (^{٣٦}) د. حسين أحمد مقداد عبد اللطيف، مصدر سابق، ص ٦٩٢.
- (^{٣٧}) محمد كاظم هادي عنجور المنصوري، مصدر سابق، ص ٥٦١.
- (^{٣٨}) (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the



Union (NIS2 Directive), Official Journal of the European Union, L 333, 27 December 2022, p.80.

(^{٣٩}) بلعروسي أمين وعبابسة حمزة، مصدر سابق، ص ٢٠٠.

(^{٤٠}) قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية المصرية، العدد ٢٨ مكرر، يوليو ٢٠٢٠.

(^{٤١}) رنا ياسين حسين، مصدر سابق، ص ٢٠٨.

(^{٤٢}) (Mostafa Ali Elokaby, op.cit, p.575.

(^{٤٣}) مصطفى كامل الشريف، نموذج تحليل الدولة الرقمية، ٢٠٢٦، مصدر سابق

(^{٤٤}) آمانج رحيم أحمد وفرمان رسول حسين، مصدر سابق، ص ٥٠.

(^{٤٥}) (International Organization for Standardization, ISO/IEC 27001:2022, Information Security Management Systems - Requirements, 3rd ed., ISO, Geneva, 2022.

(^{٤٦}) (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), Official Journal of the European Union, L 257, 28 August 2014, p.73.

(^{٤٧}) فاضل علي حسوني، مصدر سابق، ص ٤٢٢.

(^{٤٨}) (Mostafa Ali Elokaby, op.cit, p.575.

(^{٤٩}) رنا ياسين حسين، مصدر سابق، ص ٢٠٨.

(^{٥٠}) بلعروسي أمين وعبابسة حمزة، مصدر سابق، ص ٢٠٠.

(^{٥١}) (Sébastien Saunier, “La cybersécurité, un nouvel objet du droit administratif”, La Semaine Juridique Administrations et Collectivités territoriales, n° 21, 27 mai 2024, article 2144.

(^{٥٢}) د. حسين أحمد مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مصدر سابق، ص ٧٠٦.

(^{٥٣}) (Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), Défense et Sécurité des Systèmes d’Information: Stratégie de la France, Février 2011, p.7.

(^{٥٤}) (Sébastien Saunier, “La cybersécurité, un nouvel objet du droit administratif”, La Semaine Juridique Administrations et Collectivités territoriales, n° 21, 27 mai 2024, article 2144.

(^{٥٥}) حسن محمد عبد الموجود أحمد شاهين، الحماية الإدارية للنظام العام من المخاطر الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٨، يناير ٢٠٢٥، ص ٤٩٦٨.

(^{٥٦}) سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني، مجلة جامعة واسط، مجلد ٣، ٢٠٢٢، ص ٥٣٢.

(^{٥٧}) (ITU, Global Cybersecurity Agenda: National Cybersecurity Strategy Guide, International Telecommunication Union, 2015, p.22.

- (^{٥٨}) مصباح أبوبكر مصباح، دور الموظفين في تعزيز أو إضعاف أمن المعلومات بالمؤسسات، مجلة جامعة فزان العلمية، المجلد ٤، العدد ٢، يونيو ٢٠٢٥، ص ١٣٠.
- (^{٥٩}) محمد كاظم هادي عنجور المنصوري، الواقع التشريعي للأمن السيبراني في العراق، HNSJ، المجلد ٦، العدد ٨، أغسطس ٢٠٢٥، ص ٥٦١.
- (^{٦٠}) مصباح، مصدر سابق، ص ١٣٨.
- (^{٦١}) بلعروسي أمين وعباسية حمزة، مصدر سابق، ص ١٩٩.
- (^{٦٢}) حسن محمد عبد الموجود أحمد شاهين، الحماية الإدارية للنظام العام من المخاطر الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٨، يناير ٢٠٢٥، ص ٤٩٧١.
- (⁶³) (ITU, Global Cybersecurity Agenda: National Cybersecurity Strategy Guide, International Telecommunication Union, 2015, p.22
- (⁶⁴) (Jim Langevin & Mark Montgomery, "Making the Joint Cyber Defense Collaborative Work", Lawfare Media, August 6, 2021, available at: <https://www.lawfaremedia.org/article/making-joint-cyber-defense-collaborative-work>
- (⁶⁵) (Devon H. Draker, "Rethinking the Government's Role in Private Sector Cybersecurity", Student Journal of Information Privacy Law, University of Maine School of Law, February 15, 2023, Introduction, available at: <https://sjipl.minelaw.maine.edu/2023/02/15/rethinking-the-governments-role-in-private-sector-cybersecurity/>
- (⁶⁶) (Devika Sharma, Sandeep Reddy & Hamza Shahid, "Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges", Legal Studies in Digital Age (JLSDA), Vol. 2, 2024, Abstract.
- (^{٦٧}) سامر محي عبد الحمزة، مصدر سابق، ص ٥٣٢.
- (⁶⁸) (Mostafa Ali Elokaby, op.cit, p.580.

قائمة المصادر

أولاً: المصادر باللغة العربية

أولاً: الكتب

- د. زانا جلال سعيد، الموازنة بين الضبط الإداري والحريات العامة والرقابة القضائية عليها، المكتب الجامعي الحديث، الإسكندرية، ٢٠١٧.
- د. سليمان الطماوي، الوسيط في القانون الإداري، دراسة مقارنة، دار الفكر العربي، ٢٠٠٦.
- د. محمد علي عويضة، الأمن السيبراني: المفهوم التحديات والاستراتيجيات الدولية، ط ١، دار الفكر الجامعي، الإسكندرية، ٢٠٢٠.

ثانياً: البحوث والمقالات العلمية المحكمة

- أمانح رحيم أحمد وفرمان رسول حسين، نطاق سريان قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي من حيث الموضوع - دراسة مقارنة، مجلة الدراسات السياسية والأمنية، المجلد السابع، العدد الثالث، أيلول ٢٠٢٤.



- بلعروسي أمين وعبابسة حمزة، أثر الأمن السيبراني والضبط الإداري على الحقوق والحريات في العصر الرقمي، مجلة القانون والمجتمع والسلطة، العدد ١٤، ٢٠٢٥.
- حسن محمد عبد الموجود أحمد شاهين، الحماية الإدارية للنظام العام من المخاطر الإلكترونية، مجلة البحوث الفقهية والقانونية، العدد ٤٨، يناير ٢٠٢٥.
- د. حسين أحمد مقداد عبد اللطيف، دور الضبط الإداري في الحد من مخاطر الفضاء الإلكتروني في مصر وفرنسا، مجلة العلوم القانونية والاقتصادية، العدد الأول، السنة ٦٥، يناير ٢٠٢٣.
- سامر محي عبد الحمزة، السياسة التشريعية العراقية لحماية الأمن الوطني السيبراني، مجلة جامعة واسط، المجلد ٣، ٢٠٢٢.
- د. ياسر محمد عبد السلام رجب، دور الضبط الإداري في الرقابة السيبرانية وتهيئة البيئة السيبرانية الأمنة، مجلة القانون والتكنولوجيا، المجلد ١، العدد ١، أبريل ٢٠٢٢.
- فاضل علي حسوني، التوقيع الإلكتروني وحجتيه في الإثبات في ظل قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢، مجلة رسالة الحقوق، المجلد ٨، العدد ١، ٢٠١٦.
- محمد كاظم هادي عنجور المنصوري، الواقع التشريعي للأمن السيبراني في العراق: التحديات والتموّهات، مجلة العلوم الإنسانية والطبيعية (HNSJ)، المجلد ٦، العدد ٨، أغسطس ٢٠٢٥، DOI: <https://doi.org/10.53796/hnsj68/36>
- مصباح أبوبكر مصباح، دور الموظفين في تعزيز أو إضعاف أمن المعلومات بالمؤسسات، مجلة جامعة فزان العلمية، المجلد ٤، العدد ٢، يونيو ٢٠٢٥.
- م. رنا ياسين حسين، الضبط الإداري الإلكتروني في مواجهة الحريات الرقمية، مجلة العصر للعلوم الإنسانية والاجتماع، المجلد ٢٢، أبريل ٢٠٢٦، DOI: <https://doi.org/10.33193/eJHAS.22.2026.436>
- مصطفى كامل الشريف، السيادة الرقمية الغائبة وسقوط حر في المؤشرات الدولية: لماذا تراجع العراق في تصنيف EGDI و GCI؟، ٢٠٢٤، متاح على: <https://itach.dk/egdi-gci/>
- ثالثاً: التشريعات والوثائق الرسمية**
- دستور جمهورية العراق النافذ لسنة ٢٠٠٥.
- قانون التوقيع الإلكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري رقم ١٥ لسنة ٢٠٠٤، الجريدة الرسمية المصرية.
- قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية المصرية، العدد ٣٢ مكرر، أغسطس ٢٠١٨.
- قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، الجريدة الرسمية المصرية، العدد ٢٨ مكرر، يوليو ٢٠٢٠.
- قانون التوقيع الإلكتروني والمعاملات الإلكترونية العراقي رقم ٧٨ لسنة ٢٠١٢.
- قانون هيئة الاتصالات والإعلام العراقي رقم ٦٥ لسنة ٢٠٠٤.
- الاستراتيجية الوطنية المصرية للأمن السيبراني ٢٠٢٣-٢٠٢٧، المجلس الأعلى للأمن السيبراني، القاهرة، ٢٠٢٣.

ثانياً: المصادر باللغة الأجنبية

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Défense et Sécurité des Systèmes d'Information: Stratégie de la France, Février 2011.
- Devika Sharma, Sandeep Reddy & Hamza Shahid, "Cybersecurity Obligations for Critical Infrastructure: Emerging Legal Norms, Enforcement Gaps, and Governance Challenges", Legal Studies in Digital Age (JLSDA), Vol. 2, 2024.
- Devon H. Draker, "Rethinking the Government's Role in Private Sector Cybersecurity", Student Journal of Information Privacy Law, University of Maine School of Law, February 15, 2023.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive), Official Journal of the European Union, L 333, 27 December 2022.
- Elokaby, Mostafa Ali, "Development of cybersecurity laws in Egypt and its impact on the judicial system (Opportunities and challenges)", International Cybersecurity Law Review, Vol. 5, No. 4, pp. 563-584, October 2024, DOI: 10.1365/S43439-024-00132-2.
- International Organization for Standardization, ISO/IEC 27001:2022, Information Security Management Systems - Requirements, 3rd ed., ISO, Geneva, 2022.
- International Telecommunication Union (ITU), Global Cybersecurity Index 2024, Geneva, International Telecommunication Union, 2024.
- International Telecommunication Union (ITU), Global Cybersecurity Agenda: National Cybersecurity Strategy Guide, Geneva, 2015.
- Jim Langevin & Mark Montgomery, "Making the Joint Cyber Defense Collaborative Work", Lawfare Media, August 6, 2021, available at: <https://www.lawfaremedia.org/article/making-joint-cyber-defense-collaborative-work>
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), Official Journal of the European Union, L 257, 28 August 2014.
- Saunier, Sébastien, "La cybersécurité, un nouvel objet du droit administratif", La Semaine Juridique Administrations et Collectivités territoriales, n° 21, 27 mai 2024, article 2144.

