

رقابة القضاء الإداري على مشروعية المراقبة الرقمية كضمانة لحماية الحقوق والحريات العامة

The administrative judiciary's oversight of the legality of digital surveillance as a safeguard to protect public rights and freedoms

عبد الرزاق تيطراوي^{1*}، جامعة حسيبة بن بوعلي - الشلف، الجزائر، a.titraoui@univ-chlef.dz

خالد مدوي²، جامعة حسيبة بن بوعلي - الشلف، الجزائر، مخبر القانون الخاص المقارن

k.madoui@univ-chlef.dz

تاريخ قبول المقال: 2025/05/28

تاريخ إرسال المقال: 2025/01/10

الملخص:

في ظل التطور المتسارع للتكنولوجيا الرقمية، أصبحت المراقبة الرقمية وأمن المعلومات من العناصر الجوهرية في إدارة البيانات وحمايتها. وإذ تتيح هذه التقنيات إمكانيات واسعة لتعزيز الكفاءة الإدارية ومراقبة الأنشطة في المجالات العامة والخاصة، فإنها تثير في المقابل إشكالات قانونية متزايدة، لاسيما تلك المرتبطة بحماية المعطيات الشخصية وصون الحقوق والحريات الأساسية. وفي هذا الإطار، يضطلع القضاء الإداري بدور حيوي في ضبط ممارسات المراقبة الرقمية، من خلال التحقق من مدى توافقها مع الأطر القانونية الوطنية والدولية، وضمان احترام الإدارة للحقوق الفردية.

وتهدف هذه الدراسة إلى تحليل الأسس النظرية والقانونية التي تقوم عليها رقابة القضاء الإداري على مشروعية المراقبة الرقمية، مع التركيز على آليات تدخله وحدودها، ومدى فعاليتها في ضمان حماية الحقوق والحريات المكفولة للأفراد في البيئة الرقمية المعاصرة.

الكلمات المفتاحية: القاضي الإداري، المراقبة الرقمية، الرقابة القضائية، الحريات العامة.

Abstract:

In light of the rapid development of digital technology, digital surveillance and information security have become essential elements of data management and protection. While these technologies offer great potential for enhancing administrative efficiency and monitoring activities in the public and private spheres, they also raise increasing legal issues, especially those related to the protection of personal data and the safeguarding of fundamental rights and freedoms. In this context, the administrative judiciary plays a vital role in regulating digital

surveillance practices by verifying their compatibility with national and international legal frameworks and ensuring that the administration respects individual rights. This study aims to analyze the theoretical and legal underpinnings of the administrative judiciary's oversight of the legality of digital surveillance, focusing on the mechanisms and limits of its intervention, and its effectiveness in ensuring the protection of the rights and freedoms guaranteed to individuals in the contemporary digital environment.

Key words: Administrative judge, digital surveillance, Judicial control, public freedoms.

المقدمة:

في ظل التقدم التكنولوجي المتسارع الذي يشهده العالم في العصر الرقمي، أصبحت المراقبة الرقمية من أبرز القضايا التي تثير تساؤلات قانونية وأخلاقية متزايدة. فقد باتت الحكومات والهيئات المختلفة تعتمد على التقنيات الحديثة لمراقبة الأفراد، سواء لأغراض أمنية أو تنظيمية. وعلى الرغم من أن هذه الأنظمة تهدف إلى الحفاظ على النظام العام وحماية الأمن القومي، إلا أنها تطرح في المقابل إشكاليات حساسة تتعلق بحقوق الأفراد وحرياتهم الأساسية، التي أصبحت عرضة للانتهاك نتيجة التوسع في استخدام وسائل المراقبة الرقمية.

وفي هذا السياق، تبرز الحاجة الملحة إلى وضع أطر قانونية واضحة تنظم هذه الأنشطة، بما يضمن عدم المساس بالحقوق والحريات الأساسية. وهنا يبرز دور القضاء الإداري كسلطة رقابية مستقلة تعنى بحماية الأفراد وضمان التوازن بين متطلبات السلطة العامة وحقوق الإنسان في البيئة الرقمية. إذ يتولى القضاء الإداري مراقبة مشروعية القرارات والإجراءات الصادرة عن السلطات العامة، بما في ذلك تلك المتعلقة بالمراقبة الرقمية، للتحقق من مدى التزامها بالقانون وعدم تجاوزها للحدود المرسومة لها.

كما يحرص القضاء الإداري على أن يتم استخدام أدوات المراقبة ضمن إطار قانوني يراعي احترام الخصوصية وغيرها من الحقوق والحريات الدستورية، مع تمكين المتضررين من اللجوء إلى القضاء للمطالبة بالتعويض عند وقوع انتهاك. وبذلك، يسهم هذا القضاء في إرساء الضمانات القانونية الضرورية التي يجب أن تلتزم بها الجهات المعنية عند تنفيذ إجراءات المراقبة، تحقيقاً للتوازن بين متطلبات الأمن وحماية الحقوق والحريات في البيئة الرقمية.

وعليه يمكن طرح الإشكالية التالية:

إلى أي مدى يمكن للقاضي الإداري حماية حقوق الأفراد وحرياتهم في ظل المراقبة الرقمية؟

وقد اعتمدنا في هذه الدراسة المناهج التي تقتضيها هكذا مواضيع، حيث تم الاستعانة بالمنهج الوصفي الذي يعتمد على وصف الظاهرة المراد معالجتها والمنهج التحليلي من خلال تحليل النصوص القانونية المنظمة لها، بالإضافة إلى المنهج المقارن.

وفي محاولتنا الإجابة على هذه الإشكالية قمنا بتقسيم الموضوع الى مبحثين، حيث حاولنا خلال المبحث الأول التطرق إلى تحديات حماية الحقوق والحريات الأساسية في عصر المراقبة الرقمية. أما المبحث الثاني فقد تم التطرق فيه إلى الآليات الرقابية للقضاء الإداري على المراقبة الرقمية، بالإضافة إلى التطبيقات القضائية في هذا الصدد.

المبحث الأول: الأسس النظرية والقانونية لرقابة القضاء الإداري على مشروعية المراقبة الرقمية.

أحدثت التكنولوجيا الحديثة ثورة في مجال المعلومات، حيث أتاحت فرصا غير مسبوقة للوصول إلى المعرفة والتواصل وتداول المعلومات بين الأشخاص من مختلف الدول، فتطورت الجرائم العابرة للحدود وأصبحت العديد من التنظيمات الإجرامية تستخدم مختلف التقنيات الحديثة لتنفيذ مخططاتها الإجرامية، وهو ما أدى بمختلف الدول إلى فرض المراقبة على شبكات الانترنت ومحاولة تنظيم وضبط مختلف المواقع حماية لأمنها القومي والمحافظة على حقوق وحريات مواطنيها. وقد أثار هذا الموضوع عديد النقاشات حول مدى تنظيم المراقبة الرقمية مقابل حماية الحقوق الرقمية للأفراد والأمن القومي للدول.

ففي الوقت الذي تتقدم فيه هذه التقنيات بصورة رهيبية لا تزال الأطر القانونية بعيدة عن مسايرة هذا التطور التكنولوجي المتسارع.

وعليه سنطرق إلى الأسس القانونية للمراقبة الرقمية (المطلب الأول)، بالإضافة إلى الإطار القانوني لاختصاصات القضاء الإداري في رقابة مشروعية المراقبة الرقمية. (المطلب الثاني).

المطلب الأول: الأسس القانونية للمراقبة الرقمية.

بقدر ما للمراقبة الرقمية من دور في حماية الأمن القومي للدول وتنظيم ومراقبة استعمال مختلف المواقع الإلكترونية، فإنها تؤثر بشكل مباشر على حقوق الأفراد وحرياتهم، وخاصة الحق في الخصوصية وحرية التعبير وحرية التجمع، التي تعتبر من أكثر الحقوق عرضة للانتهاك جراء المراقبة الرقمية.

وفيما يلي سنبين مفهوم المراقبة الرقمية (أولا)، بالإضافة إلى الأطر القانونية المنظمة للمراقبة الرقمية الدولية والإقليمية منها، وكذا التشريعات الداخلية لمختلف الدول (ثانيا).

أولا: مفهوم المراقبة الرقمية.

تشير المراقبة الرقمية إلى استخدام الأجهزة الإلكترونية للحصول على معلومات من الاتصالات السلكية أو اللاسلكية. ويشمل ذلك التنصت على المكالمات الهاتفية، وتسجيل الفيديو، وتتبع الموقع الجغرافي، واستخراج البيانات، ورسم خرائط لوسائل التواصل الاجتماعي، ومراقبة حركة الإنترنت. وقد تتضمن المعلومات المستخلصة هوية الأطراف المعنية، ومضمون الاتصال، ودلالاته¹.

كما تشمل هذه المراقبة تتبع سلوك الأفراد وأنشطتهم من خلال استخدام البرمجيات الإحصائية وتقنيات دمج البيانات. ويمكن أن تحدث المراقبة الرقمية أيضا في سياق المحادثات الشخصية، إما عبر التنصت، أو من خلال اعتراض البيانات المنقولة بين الأجهزة البعيدة عبر الإنترنت، أو باستخدام وسائل تقنية تتيح ترجمة الانبعاثات الكهرومغناطيسية الصادرة عن الحواسيب إلى بيانات قابلة للقراءة. وإضافة إلى ما سبق، قد تتضمن المراقبة الرقمية التقاط صور أو إرسالها لشخص متواجد في مكان معين دون موافقته².

ومن أبرز أمثلة المراقبة الرقمية، تقنية التنصت الشفهي، التي تعد من أكثر أشكال المراقبة شيوعا. ويتطلب اللجوء إلى التنصت على الاتصالات الشفهية درجة عالية من الضرورة، وغالبا ما يشترط الحصول على موافقة قانونية مسبقة. ولا تقتصر سلطة التنصت على المكالمات الهاتفية فحسب، بل تمتد أيضا إلى اعتراض الرسائل النصية، ومراقبة الاتصالات عبر البريد الإلكتروني، والدرشات عبر الإنترنت، وذلك من خلال تتبع الشبكات واستخدام برمجيات متخصصة في المراقبة مثل تقنية Sniffer³. وتعتبر عمليات التنصت وسيلة فعالة للغاية في جمع الأدلة في الوقت الفعلي، إذ تتيح إمكانية التقاط الكلمات المنطوقة فعليا للمشتبه بهم، مما يعزز من قيمة الأدلة الرقمية في السياقات الأمنية أو القضائية⁴.

ثانيا: الأطر القانونية المنظمة للمراقبة الرقمية.

أصبحت المراقبة الرقمية أداة رئيسية للحكومات في مراقبة الأفراد والمجتمعات، وقد حاولت هذه الحكومات إيجاد الأطر القانونية لتنظيم عملية المراقبة الرقمية الحديثة. ومع ذلك لا تزال هناك عدة جوانب قانونية تحتاج إلى تحديث وتطوير لمواكبة هذه التحديات.

¹ Dan Kaminski, La surveillance électronique des justiciables : légitimité publique et livraison privée ? Archives de politique criminelle 2013/1 (n° 35), p 109.

² Dahmouche Faiza, The impact of the Fourth Industrial Revolution on the right to privacy, Jurisprudence Journal, Vol 61, (N°: 01- S N 33) Mars 0202, p276.

³ Sniffer هو تطبيق تم تصميمه في الأساس لمساعدة مديري شبكات الكمبيوتر، ما يفعله هو التقاط حزم البيانات التي تدور من خلال شبكة الكمبيوتر لدراساتها وتحليلها. وبهذه الطريقة، من الممكن معرفة مرسل بعض المعلومات التي يتم تداولها من خلال شبكة، ومتلقيها، والخادم الذي يتعامل مع العملية، ونوع حزمة البيانات التي يتم إرسالها.

⁴ Dan Kaminski, Op.cit., p 120.

وفيما يلي نستعرض أهم القوانين المنظمة للمراقبة الإلكترونية الدولية والإقليمية (أولاً)، بالإضافة إلى القوانين الداخلية لمختلف الدول (ثانياً).

أولاً: المواثيق الدولية والإقليمية المنظمة للمراقبة الرقمية.

تعد القوانين الدولية المنظمة للمراقبة الإلكترونية مجموعة من الاتفاقيات والمواثيق التي تهدف إلى تنظيم استخدام تقنيات المراقبة الإلكترونية، وذلك في إطار حماية حقوق الإنسان وضمان الحق في الخصوصية. وفي هذا السياق، أصدرت العديد من الهيئات الدولية والإقليمية قرارات ومواثيق تهدف إلى حماية حقوق الإنسان في ظل التوسع المتزايد في استخدام أدوات المراقبة الرقمية من قبل العديد من الحكومات.

1- قرار الأمم المتحدة لسنة 2023:

اعتمدت الجمعية العامة للأمم المتحدة القرار رقم 298/77 الصادر في 22 يونيو 2023، والمتعلق بالاستعراض الثامن لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، والتي تم تبنيها لأول مرة عام 2006 بموجب القرار رقم 288/60. وتتضمن هذه الاستراتيجية مجموعة من الأهداف والإجراءات الرامية إلى القضاء على الإرهاب وتعزيز التعاون الدولي في مواجهته¹.

وقد تم التأكيد في هذا السياق على أن مكافحة الإرهاب يجب أن تمارس بما يتماشى مع احترام حقوق الإنسان، لا سيما في ظل التحديات المستجدة التي برزت خلال السنوات الأخيرة، مثل الهجمات السيبرانية، واستخدام شبكة الإنترنت لنشر الفكر المتطرف، بما في ذلك عبر منصات التواصل الاجتماعي. كما شددت الاستعراضات المتعاقبة على أنه لا يجوز تبرير انتهاك حقوق الأفراد بذريعة مكافحة الإرهاب.

وعلى الرغم من أن استراتيجية الأمم المتحدة لمكافحة الإرهاب قد أحرزت تقدماً ملموساً في التصدي للتهديدات الإرهابية على الصعيد العالمي، فإن تحقيق التوازن بين متطلبات الأمن القومي وضمان حماية حقوق الإنسان لا يزال يشكل تحدياً دائماً. ويتطلب هذا التحدي التزاماً فعلياً من الدول الأعضاء باحترام حقوق الإنسان في جميع مراحل تنفيذ سياسات مكافحة الإرهاب، بما في ذلك استخدام تقنيات المراقبة الحديثة.

2- تقارير المفوضية السامية لحقوق الإنسان لسنة 2022:

¹ قرار الجمعية العامة للأمم المتحدة رقم A/RES/60/288 الصادر في 8 سبتمبر 2006 والمتعلق باستراتيجية الأمم المتحدة لمكافحة الإرهاب والقرار رقم A/RES/77/298 والمتعلق بالاستعراض الثامن من الموقع: <https://www.un.org/ar/ga/77/resolutions.shtml> تاريخ الاطلاع عليه: 15 نوفمبر 2024 على الساعة: 21:24.

في 12 مايو 2022، صدر التقرير الأول بشأن حجب الإنترنت وتداعياته القانونية وانعكاساته على حقوق الإنسان، تنفيذاً لقرار مجلس حقوق الإنسان رقم 16/47. ويهدف هذا التقرير إلى تسليط الضوء على مسألة حجب الإنترنت ومدى تأثيرها على حقوق الأفراد وحرياتهم، وفي مقدمتها الحق في حرية التعبير¹. وصدر عن الهيئة ذاتها في 7 أكتوبر 2022 تقرير ثانٍ يتعلق بتعزيز حماية الحق في الخصوصية في الفضاء الرقمي، حيث تناول بالتفصيل آثار المراقبة الرقمية على الحق في الخصوصية والحقوق المرتبطة به. وقد اختتم التقرير بجملة من التوصيات الموجهة إلى الدول، أبرزها ضرورة ضبط استخدام تقنيات المراقبة الرقمية وفقاً لأحكام القانون الدولي لحقوق الإنسان، ولا سيما احترام مبادئ الشرعية، والضرورة، والتناسب في كل إجراء رقابي يتخذ.

3- اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي:

اللائحة رقم 679/2016، الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016، بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، دخلت حيز التنفيذ في 25 مايو 2018². وتتضمن هذه اللائحة قواعد ملزمة تنظم كيفية استخدام المنظمات والشركات للبيانات الشخصية بشكل قانوني ومشروع. وقد نصت على العديد من الالتزامات المفروضة على الحكومات والشركات، إلى جانب مجموعة من الضمانات التي تكفل حماية حقوق الأفراد في مواجهة الجهات المسؤولة عن معالجة بياناتهم الشخصية. ويجب، وفقاً لأحكام هذه اللائحة، أن يتم استخدام البيانات الشخصية بطريقة قانونية، وبما يراعي حقوق الأفراد ويحترم خصوصيتهم.

ثانياً: القوانين الوطنية المنظمة للمراقبة الرقمية.

تختلف القوانين الوطنية المتعلقة بالمراقبة الإلكترونية من دولة إلى أخرى، حيث تحدد قواعد المراقبة بناءً على الإيديولوجية السياسية والاجتماعية والأمنية، إضافة إلى مدى احترام حقوق الإنسان والحريات العامة.

1- القوانين الأوروبية والأمريكية:

¹ تقرير المفوضية السامية لحقوق الإنسان رقم A/HRC/50/55 الصادر بتاريخ: 13 ماي 2022 منشور على الموقع: <https://www.ohchr.org/ar/stories/2022/06/switching-internet-causes-incalculable-damage-un-report>

تاريخ الاطلاع عليه: 21 نوفمبر 2024. على الساعة: 19:25.

² Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018. The European Data Protection Regulation is applicable as of May 25th, 2018 in all member states to harmonize data privacy laws across Europe.

في هذا السياق أقرت الحكومة الأمريكية عدة تشريعات، نذكر منها قانون حماية الخصوصية على الإنترنت، ويحكم هذا القانون المراقبة الإلكترونية المتعلقة بالبريد الإلكتروني والبيانات المخزنة في قواعد البيانات الإلكترونية. كما يحدد الضوابط التي يجب على الحكومة اتباعها قبل إجراء المراقبة.

وقد سن الكونغرس الأمريكي قانون خصوصية الاتصالات الإلكترونية لعام 1986 (ECPA) لتوسيع القيود المفروضة على التنصت الحكومي على المكالمات الهاتفية لتشمل نقل البيانات الإلكترونية عبر الحواسيب. يحظر القانون التنصت المتعمد، سواء الفعلي أو محاولة التنصت، بالإضافة إلى الاستخدام أو الاعتراض أو محاولة اعتراض أي اتصال سلكي أو شفوي أو إلكتروني. كما يمنع استخدام الاتصالات التي تم الحصول عليها بطرق غير قانونية¹. ويضمن القانون حماية خصوصية محتويات الملفات المخزنة لدى مقدمي الخدمة، والسجلات التي يحتفظ بها هؤلاء المزودون عن المشتركين، ويفرض على الجهات الحكومية ضرورة الحصول على أمر قضائي يجيز تركيب واستخدام أجهزة تسجيل المكالمات والتعقب.

أما في فرنسا، فإن أهم قانون يتعلق بالمراقبة الرقمية هو قانون الجمهورية الرقمية، الذي تم تبنيه في 7 أكتوبر 2016. يهدف هذا التشريع إلى تعزيز حقوق المواطنين في الفضاء الرقمي وضمان الشفافية في إدارة البيانات وحمايتها. ويعد هذا القانون خطوة هامة نحو تحديث التشريعات الفرنسية لمواكبة التغيرات التكنولوجية المتسارعة في عالم الإنترنت والبيانات الرقمية². يتضمن القانون إجراءات تهدف إلى حماية الأفراد من تتبع أنشطتهم عبر الإنترنت من قبل الشركات، حيث يلزم المواقع الإلكترونية بالحصول على موافقة صريحة من المستخدمين قبل جمع البيانات أو تتبع سلوكهم على الشبكة.

وفي المملكة المتحدة، صدر قانون صلاحيات التحقيق (Investigatory Powers Act 2016)، وهو تشريع أقره البرلمان البريطاني يمنح الحكومة سلطات واسعة النطاق في مجال المراقبة. يهدف القانون إلى تنظيم كيفية قيام وكالات الاستخبارات ووكالات إنفاذ القانون والجهات الحكومية الأخرى بإجراء المراقبة والوصول إلى البيانات لأغراض الأمن القومي، والوقاية من الجريمة، وجمع المعلومات الاستخباراتية. ويخول هذا القانون الأجهزة الأمنية صلاحيات واسعة في مجال المراقبة الإلكترونية، بما في ذلك القدرة على اعتراض البيانات عبر الإنترنت وحفظها لمدة تصل إلى عامين³.

¹ Electronic Communications Privacy Act of 1986, H.R.4952 — 99th Congress (1985-1986), The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008.

² LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.

³ Investigatory Powers Act 2016, UK Public General Acts 2016 c. 25.

أما في ألمانيا فتم إصدار قانون حماية البيانات الفيدرالي (BDSG) في 30 جوان 2017¹، حيث ينص القسم 83 منه على الأضرار والتعويضات. إذ إذا تسبب المراقب في ضرر لصاحب البيانات نتيجة معالجة البيانات الشخصية بطريقة غير قانونية، سواء بموجب هذا القانون أو بموجب لوائح أخرى تنطبق على المعالجة، فإنه يلزم بدفع تعويض لصاحب البيانات.

2- القوانين العربية:

استجابة للتغيرات التي شهدتها جوانب الحياة المختلفة نتيجة التطور التكنولوجي المتسارع، حاولت العديد من الدول العربية مواكبة التحولات التي شهدتها القوانين المقارنة، من خلال إصدار تشريعات تهدف إلى تنظيم المراقبة الإلكترونية بما يضمن حماية حقوق الأفراد وحرياتهم الأساسية.

وفي هذا الإطار، أصدرت مصر قانون مكافحة الإرهاب رقم 94 لسنة 2015، الذي تم تعديله في عام 2017 لمواكبة التحديات الأمنية المتزايدة، خاصة في ظل تصاعد العمليات الإرهابية في بعض المناطق بمصر. يسمح القانون بمراقبة الأشخاص المتهمين بالإرهاب عبر وسائل مثل التنصت على المكالمات، ومراقبة الحسابات الإلكترونية، وغيرها من وسائل المراقبة الرقمية².

أما في الإمارات، فقد صدر قانون الجرائم الإلكترونية لسنة 2021، الذي ينظم الأنشطة الإلكترونية ويجرم استخدام وسائل الاتصال أو الإنترنت في نشر محتوى يمس الأمن القومي. يسمح القانون للسلطات بمراقبة الإنترنت ومراجعة البيانات الشخصية للأفراد في إطار مكافحة الجرائم الإلكترونية³.

أما المشرع الجزائري، فقد سار على خطى نظرائه من الدول العربية بإصدار بعض التشريعات التي تندرج في هذا السياق، حيث صدر سنة 2009 القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. تضمن هذا القانون الأحكام والضوابط المنظمة للمراقبة الإلكترونية في الفصل الثاني المعنون بـ«مراقبة الاتصالات الإلكترونية»، حيث حددت المادة 04 الحالات التي يمكن فيها اللجوء إلى عملية المراقبة. كما قيد المشرع عملية المراقبة بضرورة الحصول على إذن مكتوب من السلطة القضائية المختصة، وهو ما يعد ضمانة مهمة لتعزيز حماية خصوصية الأفراد⁴.

¹ قانون حماية البيانات الفيدرالي الصادر في 30 يونيو 2017 (BGBl. I p. 2097)، والذي تم تعديله آخر مرة بموجب المادة 7 من قانون 6 مايو 2024 (BGBl. 2024 I No. 149).

² القانون رقم 94 لسنة 2015، الجريدة الرسمية العدد 33 مكرر الصادرة في 15 أوت 2015.

³ مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، دخل حيز التنفيذ اعتبارا من 02 يناير 2022.

⁴ القانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 14 الصادرة في 16 أوت 2009.

كما تم أيضا إصدار القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي¹، حيث ينظم هذا القانون كيفية جمع البيانات الشخصية واستخدامها، ويضع قيودا على الوصول إليها أو معالجتها من قبل أطراف ثالثة. كما يشترط موافقة الأفراد على جمع بياناتهم الشخصية، ويشدد على أن أي مراقبة إلكترونية يجب أن تكون خاضعة لرقابة السلطات القضائية المختصة، وتتم في إطار قانوني وضمن نطاق محدد².

وما يمكن قوله في هذا الصدد، هو أنه على الرغم من وجود قوانين تنظم المراقبة الإلكترونية في الجزائر، فإن بعض التحديات لا تزال قائمة، خصوصا فيما يتعلق بالتطبيق الفعلي لتلك القوانين بما يضمن عدم انتهاك خصوصية الأفراد.

وتبذل الحكومات جهودا كبيرة لوضع أطر قانونية تنظم عملية المراقبة الرقمية بما يحقق التوازن بين حماية الأمن القومي وكفالة الحقوق والحريات الأساسية للأفراد. غير أن التساؤل يظل مطروحا بشأن مدى قدرة هذه التشريعات على مواكبة التطور السريع والمتسارع للتقنيات الرقمية الحديثة.

المطلب الثاني: الإطار القانوني لاختصاصات القضاء الإداري في رقابة مشروعية المراقبة الرقمية.

في ظل التطور التكنولوجي المتسارع، وازدياد اعتماد الإدارة على وسائل المراقبة الرقمية، برزت الحاجة الملحة إلى إطار قانوني واضح يحدد اختصاصات القضاء الإداري في رقابة مشروعية هذه الممارسات، باعتبار هذه الرقابة أداة أساسية لضمان حماية حقوق الأفراد وحرياتهم العامة.

وعليه سنتطرق إلى الأسس القانونية التي يستمد منه اختصاص القضاء الإداري في هذا السياق (أولا)، بالإضافة إلى تحديد الجهات القضائية المعنية (ثانيا)، ونطاق الرقابة التي تباشرها، سواء من حيث الشروط الشكلية أو الموضوعية، وصولاً إلى حدود الرقابة القضائية على المراقبة الرقمية (ثالثا).

أولاً: الأسس القانونية للرقابة القضائية على المراقبة الرقمية.

يستند اختصاص القاضي الإداري في الرقابة على المراقبة الرقمية إلى مبدأ أساسي يتمثل في مبدأ المشروعية، الذي يفرض على الإدارة الالتزام بالقانون وعدم الخروج عنه في جميع تصرفاتها، بما في ذلك التدخلات التي

¹ القانون رقم 18-07 المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، صادرة في 12 يونيو 2018.

² وتعزيزا لهذا القانون تم سنة 2022 إنشاء اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي، والتي تضطلع بمهام الرقابة السابقة واللاحقة لعملية معالجة المعطيات الشخصية، بموجب المرسوم الرئاسي رقم 22-187 المؤرخ في 18 ماي 2022 يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، الصادرة في 20 ماي 2022.

تتم عبر الوسائل الرقمية الحديثة. وينبثق هذا الاختصاص من عدة مصادر قانونية تشكل مجتمعة الإطار المرجعي لهذه الرقابة، وفي مقدمتها النصوص الدستورية، التي تركز في معظم الدول الديمقراطية مجموعة من الحقوق الأساسية، مثل حرية التعبير، والحق في الخصوصية، وسرية المراسلات، وهي حقوق تشمل أيضا وسائل الاتصال الإلكترونية. وبموجب هذه الضمانات الدستورية، يتولى القضاء الإداري مسؤولية التحقق من مدى احترام الإدارة لتلك الحقوق عند استخدامها لأدوات المراقبة الرقمية، بما يضمن توافق ممارساتها مع المبادئ القانونية المستقرة¹.

فعلى سبيل المثال، تنص المادة 47 من الدستور الجزائري وفقاً لتعديل سنة 2020 على أن "حياة المواطن الخاصة محمية ولا يجوز انتهاكها"، كما تنص على "حماية سرية المراسلات ووسائل الاتصال"، وهو ما يعد أساساً دستورياً هاماً يمكن القضاء الإداري من ممارسة رقابته على مشروعية تدخلات الإدارة في الفضاء الرقمي².

وفي السياق ذاته، تعد المواثيق الدولية لحقوق الإنسان من المصادر الجوهرية التي يستند إليها القاضي الإداري، حيث توفر اتفاقيات دولية مثل العهد الدولي الخاص بالحقوق المدنية والسياسية (المادة 17) والاتفاقية الأوروبية لحقوق الإنسان (المادة 8) معايير قانونية موضوعية لتقييم مدى شرعية تدخل الإدارة في الحياة الخاصة للأفراد من خلال استخدام الوسائل الرقمية.

وعلاوة على ذلك، أصدرت معظم الدول تشريعات وطنية خاصة بحماية المعطيات الشخصية، تفرض التزامات صارمة على الهيئات الإدارية فيما يتعلق بجمع البيانات الشخصية وتخزينها ومعالجتها، بما يضمن احترام الخصوصية والحقوق الأساسية للأفراد.

ثانياً: الجهات القضائية المختصة ونطاق الرقابة.

تتنوع الهيئات القضائية الإدارية المكلفة برقابة المراقبة الرقمية، تبعاً للنظام القضائي المعتمد في كل دولة. ففي الأنظمة التي تعتمد قضاء إدارياً مستقلاً، كما هو الحال في فرنسا، يتولى مجلس الدولة مهمة الرقابة على قرارات الإدارة، بما في ذلك تلك المرتبطة باستخدام أدوات المراقبة الرقمية، وذلك في إطار احترام مبدأ مشروعية وحماية الحقوق الأساسية³.

¹ خليل أحمد، القضاء الإداري وحماية الحريات الأساسية، دار الجامعة الجديدة، 2021، ص 133.

² المرسوم الرئاسي رقم 442-20 المؤرخ في 20 ديسمبر 2020 المتضمن التعديل الدستوري لسنة 2020، ج ر عدد 82 المؤرخة في 30 ديسمبر 2020.

³ Mantelero, Alessandro, The Future of Data Protection: Digital Surveillance and Administrative Law, Springer, 2018, p 98.

وفي بعض الدول الأخرى، مثل ألمانيا، توجد محاكم إدارية متخصصة تنظر في النزاعات المتعلقة بالمراقبة الإلكترونية وحماية الخصوصية الرقمية، مما يمكن من ضمان رقابة أكثر فاعلية ودقة في هذا المجال. إلى جانب ذلك، تضطلع بعض الهيئات شبه القضائية، مثل سلطات حماية البيانات، بدور رقابي بالغ الأهمية، من خلال إصدار قرارات وتوصيات تتعلق بمدى احترام قواعد حماية البيانات الشخصية، وتعد هذه القرارات قابلة للطعن أمام القضاء الإداري، ما يعزز من فعالية الرقابة القانونية على الممارسات الرقمية التي قد تمس حقوق الأفراد¹.

ويشمل نطاق رقابة القاضي الإداري على المراقبة الرقمية مستويات متعددة، تبدأ أولاً بالرقابة الشكلية، حيث يتحقق القاضي من مدى احترام الإدارة للإجراءات القانونية المقررة قبل الشروع في تنفيذ عملية المراقبة، وفي مقدمتها ضرورة الحصول على إذن مسبق من جهة مختصة.

ثم تأتي الرقابة الموضوعية، التي تقوم على فحص مبدأي الضرورة والتناسب، أي التأكد من أن الوسيلة الرقمية المستخدمة في المراقبة متلائمة مع الهدف المشروع، دون أن تشكل مساساً مفرطاً أو غير مبرر بحقوق الأفراد. وفي هذا الإطار، يُراقب القضاء الإداري مدى احترام الإدارة لحرمة الحياة الخاصة، وضمان عدم جمع المعلومات أو تتبع الأفراد عبر الوسائل التقنية إلا ضمن شروط قانونية واضحة ومقيدة².

وأخيراً، تمتد الرقابة لتشمل تقييم فعالية الضمانات الإجرائية المقررة لحماية الأفراد، مثل الحق في الإعلام وحق الطعن، بالإضافة إلى وجود آليات رقابة ذاتية ومؤسسية فعالة داخل الهيئات الإدارية، لضمان عدم التعسف في استخدام أدوات المراقبة الرقمية³.

ثالثاً: حدود الرقابة القضائية على المراقبة الرقمية.

رغم اتساع صلاحيات القضاء الإداري في الرقابة على أعمال الإدارة، إلا أن هناك حدوداً جوهرية، خاصة في حالات الطوارئ وأعمال السيادة التي تمنح الإدارة صلاحيات استثنائية قد تقيد تدخل القاضي. في العديد من الدول، تسمح التشريعات للأجهزة الأمنية بالمراقبة الرقمية سرا لحماية الأمن القومي، مما يحد من صلاحيات القاضي الإداري بسبب السرية حول الأدلة والتقنيات المستخدمة. هذا يقيد فعالية الرقابة القضائية ويثير تساؤلات حول كيفية تحقيق التوازن بين الأمن وحماية الحقوق دون المساس بالسرية الأمنية. في حالات

¹ Nolte, Georg, Federal Administrative Courts and Digital Surveillance in Germany, European Public Law, 2021, p 45.

² Lenaerts, Koen. Digital Rights and Administrative Oversight, CMLR, Vol. 58, 2021, p. 367.

³ Mantelero, Alessandro, Op.cit, p 132.

الطوارئ، يواجه القاضي تحدياً في تقييم ضرورة المراقبة الرقمية ومدى التزامها بمبدأي الضرورة والتناسب، خاصة مع صعوبة الوصول إلى الأدلة بسبب السرية¹.

المبحث الثاني: الآليات الرقابية للقضاء الإداري على المراقبة الرقمية.

تعد الرقابة القضائية إحدى أبرز الضمانات الفاعلة للحد من تجاوزات السلطات التنفيذية في استخدام أدوات المراقبة الرقمية، كما تساهم بشكل فعال في تعزيز حماية الحقوق الأساسية في ظل التحولات التقنية المعاصرة، عبر تحقيق التوازن الدقيق بين متطلبات الأمن وضرورات حفظ الحريات والحقوق الفردية. ومع التوسع في الاعتماد على التقنيات الرقمية ضمن تطبيقات الأمن القومي وحماية النظام العام، أصبحت الرقابة القضائية في هذا المجال أكثر من ضرورية.

وفيما يلي سنتطرق إلى دور القضاء الإداري في رقابة مشروعية المراقبة الإلكترونية (المطلب الأول)، وكذا استعراض بعض التطبيقات القضائية لرقابة القضاء الإداري على المراقبة الرقمية (المطلب الثاني).

المطلب الأول: دور القضاء الإداري في رقابة مشروعية المراقبة الرقمية.

مع تزايد استخدام المراقبة الرقمية، تبرز العديد من القضايا القانونية المتعلقة بحقوق الأفراد وحرياتهم الشخصية، مثل الحق في الخصوصية وحماية البيانات الشخصية. هذا الأمر يقتضي وجود رقابة قضائية على السلطات العامة في هذا المجال، فيتدخل القضاء الإداري لتنظيم مشروعية هذه الممارسات (أولاً)، بالإضافة إلى سلطاته في تقدير التعويض للمتضررين من إجراءات المراقبة (ثانياً).

أولاً: رقابة مشروعية القرارات الإدارية المتعلقة بالمراقبة الرقمية.

يتولى القضاء الإداري رقابة مشروعية القرارات الإدارية المتعلقة باستخدام المراقبة الرقمية، حيث لا تقتصر هذه الرقابة على فحص مدى تطبيق القانون فحسب، بل تشمل أيضاً التأكد من مراعاة حقوق الأفراد وحرياتهم العامة. يتدخل القاضي الإداري للتحقق من أن هذه القرارات تتخذ ضمن إطار قانوني واضح، وتتناسب مع الضرورة والملاءمة، بما يضمن التوازن بين متطلبات الأمن وحقوق الأفراد وحرياتهم.

1- الرقابة على الأساس القانوني للقرار الإداري:

الأساس القانوني للقرار الإداري هو الركيزة الأولى التي يقيم عليها القاضي الإداري مشروعية القرارات المتعلقة بالمراقبة الرقمية. يتعين على الإدارة اتخاذ قرارات المراقبة بناء على قوانين صريحة وواضحة تمنحها هذا الحق. فمثلاً في حالة المراقبة الجماعية أو جمع البيانات الشخصية، يتعين أن تستند هذه القرارات إلى قوانين مكافحة

¹ Oreste Pollicino, The Transatlantic Dimension of the Judicial Protection of Fundamental Rights Online, the Italian review of international and comparative law 1 (2021), p 284.

الإرهاب أو الأمن القومي، وتكون هذه القوانين متوافقة مع المعايير الدولية لحقوق الإنسان. وإذا كانت الإدارة تتخذ قرارات دون تفويض قانوني صريح، يحق للقاضي الإداري إلغاء هذه القرارات باعتبارها غير مشروعة¹. في حال حدوث تدخلات غير مشروعة، مثل المراقبة التي لا تستند إلى تفويض قضائي أو التي تتعدى حدود الضرورة، يجب أن يتمكن الأفراد من اللجوء إلى القضاء للطعن في هذه الإجراءات. فالقضاء الإداري بما لديه من سلطة، يمكنه إيقاف العمليات غير القانونية أو منح تعويضات للمتضررين. ومن أمثلة ذلك نجد قرار المحكمة الفدرالية السويسرية في قضية استخدام نظام آلي لتفتيش المركبات ومراقبة حركة المرور، حيث يعتمد هذا النظام على دمج البيانات مع تلك الموجودة في ملفات أخرى ومقارنتها بطريقة آلية تسمح بالمعالجة التسلسلية. وقد رأت المحكمة أن إجراء التسجيلات وتخزينها بواسطة نظام المراقبة هذا ينتهك الحقوق الأساسية للأشخاص المعنيين وخاصة الحق في الخصوصية². وكمثال آخر حكم المحكمة الأوروبية لحقوق الإنسان الصادر في 01 ديسمبر 2015 في قضية حجب المواقع الإلكترونية في تركيا. وزعم مقدمو الطلب، بمن فيهم المدونون ومستخدمو الإنترنت، أن حجب بعض المواقع الإلكترونية ينتهك حقهم في حرية التعبير. ووجدت المحكمة أن التدابير التي اتخذتها السلطات التركية لم تكن مبررة بشكل كاف وانتهكت المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان. وأكد الحكم على ضرورة فرض قيود واضحة وشفافة ومحددة بدقة من أجل احترام حرية التعبير³.

2- الرقابة على مدى التناسب والضرورة:

تتمثل إحدى أهم جوانب الرقابة القضائية في التحقق من أن القرارات الإدارية المتعلقة بالمراقبة الرقمية تتماشى مع مبدأ التناسب والضرورة، حيث تمتلك الإدارة السلطة التقديرية لاتخاذ إجراءات المراقبة وفقا لمتطلبات حفظ النظام العام والمحافظة على الأمن القومي. في هذا السياق، يجب أن يتحقق القاضي الإداري من أن المراقبة لا تفرط في انتهاك حقوق الأفراد، وأنها ضرورية لتحقيق الهدف المشروع (مثل مكافحة الإرهاب أو الجريمة). بمعنى آخر، ينبغي أن يكون التدخل في حقوق الأفراد، مثل المراقبة الجماعية أو مراقبة البيانات الرقمية، هو الحل الأقل تدخلا لتحقيق الهدف المنشود⁴.

¹ Electronic Surveillance and Civil Liberties, Federal Government Information Technology: (Washington, DC: U.S. Congress, Office of Technology Assessment, OTACIT-293, October 1985), p18.

² Johan Wolswinkel, Intelligence artificielle et droit administratif, édition du conseil de l'Europe, décembre, 2022, p24.

³ European Court of Human Rights, Cengiz and others v. Turkey (applications No. 48226/10 and No. 14027/11), judgment of 1 December 2015; and Ahmet Yikdirim v. Turkey (application No. 3111/10).

⁴ علي دلشاد معروف، رقابة القضاء على مشروعية قرارات الضبط الإداري، الطبعة 0، مكتبة وفاء القانونية، الإسكندرية، مصر، 2016، ص 234.

على سبيل المثال، إذا كان بالإمكان استخدام طرق أقل تدخلا مثل الحصول على إذن قضائي لمراقبة شخص محدد، فلا يجوز اتخاذ إجراءات موسعة أو جماعية لمراقبة جميع الأفراد. إذا تبين أن الإجراءات الإدارية لم تكن متناسبة أو ضرورية، فإن القاضي الإداري قد يعتبر القرار غير قانوني ويقضي بإلغائه. وكمثال على ذلك حكم المحكمة الأوروبية لحقوق الإنسان في قضية تتعلق بحجب المواقع الإلكترونية والقيود المفروضة على حرية التعبير على الإنترنت في روسيا. وقد طعن مقدم الطلب، وهو فرد روسي، في حجب المواقع الإلكترونية من قبل السلطات الروسية، بحجة أن ذلك ينتهك حقه في حرية التعبير بموجب المادة 10 من الاتفاقية الأوروبية لحقوق الإنسان. وقد فحصت المحكمة مبررات القيود ووجدت أنها غير متناسبة في هذه الحالة، مؤكدة على أهمية حرية تلقي المعلومات¹.

3- الرقابة على الإجراءات المتبعة:

يتمثل دور القضاء في مراقبة ما إذا كانت الإدارة قد اتبعت الإجراءات القانونية المناسبة قبل تنفيذ هذه المراقبة، مثل الحصول على إذن قضائي أو إبلاغ الأفراد المعنيين بشأن هذه الإجراءات. كما يقوم القضاء الإداري بمراجعة ما إذا كانت هناك ضوابط واضحة تحد من استخدام المراقبة، بما في ذلك تحديد أهدافها، وأماكن تنفيذها، ومدى التناسب بين الهدف من المراقبة والوسائل المستخدمة، بالإضافة إلى الرقابة على الغاية التي تهدف السلطات إلى تحقيقها من هذه المراقبة والتي تتمثل في حفظ النظام وحماية الأمن القومي وحقوق الإنسان².

وقد يتدخل القضاء الإداري بتوجيه أوامر للإدارة في حالة ما اتخذت موقفا سلبيا أو امتنعت عن التدخل لحماية حقوق الأفراد متى كان القانون يلزمها بذلك (القرارات السلبية)، وكمثال على ذلك نجد قرار نهائي بات المحكمة الإدارية العليا في مصر المؤيد لحكم محكمة القضاء الإداري في قضية حجب موقع "يوتيوب" لمدة شهر بعد عرض فيلم مسيء للرسول عليه الصلاة والسلام، هذا القرار يلزم تدخل جهة الإدارة المتمثلة في الجهاز القومي لتنظيم الاتصالات لحماية حرمة المعتقدات الدينية الإسلامية³. حيث اعتبرت المحكمة الإدارية العليا أن حماية الأمن الاجتماعي مقدم على حرية الرأي والتعبير وهو المصلحة الأولى بالرعاية، وأنه لا مجال للموازنة بين الأمن القومي وأي اعتبارات أخرى.

ثانيا: سلطات القاضي الإداري في تقدير التعويض عن أضرار المراقبة الرقمية.

¹ European Court of Human Rights, Vladimir Kharitonov v. Russia (Application No. 10795/14), Judgment of 23 June 2020, para. 46

² محمد رشاد الأمامي، القرار الإداري الإلكتروني وأوجه الرقابة عليه، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، 2023، ص30.

³ حكم المحكمة الإدارية العليا المصرية الصادر في 25 ماي 2018 في القضية رقم 60693 لسنة 66 ق، حيث الدعوى أمام الدائرة الثانية لمحكمة القضاء الإداري في 18 سبتمبر 2012.

قد تؤدي المراقبة الرقمية إلى وقوع أضرار وخاصة إذا كانت المراقبة غير قانونية أو مبالغ فيها، وهو ما يمنح للمتضررين الحق في المطالبة بتعويضات. وفي هذا السياق، يلعب القضاء الإداري دورا مهما في حماية حق الأفراد في المطالبة بالتعويضات المناسبة للأضرار التي قد تصيبهم. وتتعدد سلطات القاضي الإداري في تقدير التعويضات، حيث يتمتع بسلطة تقديرية كبيرة في تحديد مدى الأضرار التي تعرض لها الأفراد نتيجة المراقبة الرقمية. هذه الأضرار يمكن أن تكون مادية أو معنوية.

ويعتمد عليها القاضي الإداري في تقدير التعويض على نوع الضرر وتقديره، حيث يجب على القاضي الإداري أن يحدد نوع الأضرار التي لحقت بالمتضرر نتيجة المراقبة الرقمية. قد تتفاوت الأضرار من حالة إلى أخرى، فقد تشمل الأضرار المادية مثل الخسائر المالية الناتجة عن إفشاء المعلومات الشخصية أو استخدامها في غير محلها، أو قد تكون أضرارا معنوية مثل التوتر النفسي، أو الأثر على الحياة الشخصية والعائلية بسبب انتهاك الخصوصية أو التهديد باستمرار المراقبة.

وقد يقوم القاضي الإداري في تقدير التعويض عن طريق تحديد مدى تأثير المراقبة الرقمية على حقوق المتضرر. فإذا كانت المراقبة قد أثرت بشكل كبير على حياة الشخص الخاصة أو حريته في التعبير أو التنقل، فإن القاضي قد يقرر تعويضا أكبر. على سبيل المثال، إذا كانت المراقبة قد تسببت في فقدان الوظيفة أو الإضرار بالعلاقات الشخصية، فإن ذلك يشكل أساسا قويا لتقدير تعويض كبير¹.

يتمتع القاضي الإداري بسلطة تقدير قيمة التعويض بناء على عدة معايير تتعلق بحجم الأضرار الناتجة عن المراقبة الرقمية. القاضي قد يقرر تعويضا ماليا محددا أو تعويضا عينيا إذا كان ذلك مناسبا لحالة القضية. غير أنه في بعض الحالات، قد يتعين على القاضي الإداري التعامل مع قضايا تتعلق بعدد كبير من الأفراد الذين تعرضوا للمراقبة الرقمية، مثل حالات المراقبة الجماعية².

ومن أهم المعايير الرئيسية التي يعتمد عليها القاضي الإداري هو مبدأ التناسب. هذا يعني أن التعويض الذي يقره القاضي يجب أن يتناسب مع حجم الأضرار التي لحقت بالمتضرر. ويشمل مبدأ التناسب أيضا عدم الإفراط في تقدير التعويضات بحيث لا تكون غير مناسبة للضرر الفعلي الذي وقع.

ورغم ذلك قد تواجه القاضي الإداري بعض الصعوبات، خاصة تلك المتعلقة بإثبات الضرر الرقمي، فغالبا ما تكون الأدلة المتعلقة بكيفية حدوث المراقبة أو البيانات التي تم جمعها غير متاحة للأفراد. كما أن التقنيات

¹ زعزوعة فاطمة، أساس المسؤولية الإدارية عن أضرار المعالجة الآلية لمعطيات المرفق الإلكتروني، مجلة الدراسات القانونية والاقتصادية، المجلد 04، العدد 03، 2021، ص 541-542.

² العربي وردية، أساس الضرر الموجب للتعويض في مجال المسؤولية المدنية للدولة ودور القاضي الإداري في تقدير التعويض الخاص به، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 06، العدد 02، 2023، ص 209-210.

التي تستخدمها الحكومات في المراقبة قد تكون معقدة لدرجة أن الأفراد لا يستطيعون دائما معرفة ما إذا كانوا قد تعرضوا للمراقبة بالفعل أو نوعية الأضرار التي لحقت بهم. لهذا يكون عبء إثبات الضرر في قضايا المراقبة الرقمية أكبر، مما يعيق قدرة الأفراد على المطالبة بحقوقهم. بالإضافة إلى صعوبة تحديد الأضرار المعنوية، حيث أن الأضرار النفسية أو الاجتماعية الناتجة عن المراقبة الرقمية قد تكون أكثر صعوبة في التقييم. فالقاضي قد يحتاج إلى الأدلة والشهادات من الخبراء النفسيين أو محامي الدفاع لشرح تأثير المراقبة على حياة الفرد.

إن تعويض المتضررين من المراقبة الإلكترونية يعد أمرا بالغ الأهمية لضمان حماية حقوق الأفراد وحرياتهم الأساسية. ويتطلب ذلك وجود آليات قانونية واضحة تتيح للأفراد تقديم دعاوى قضائية للحصول على تعويضات في حال تم انتهاك حقوقهم بسبب المراقبة غير القانونية. في الوقت نفسه، يجب أن تعمل الهيئات القضائية الوطنية والدولية على ضمان أن تتماشى السياسات المتعلقة بالمراقبة مع المعايير الدولية لحقوق الإنسان، مع توفير تعويضات فعالة للمتضررين.

المطلب الثاني: التطبيقات القضائية لرقابة القضاء الإداري على المراقبة الرقمية.

في ظل الانتهاكات المتزايدة للحقوق والحريات العامة جراء الاستخدام الواسع النطاق لتقنيات المراقبة الرقمية الحديثة، برز دور القضاء الإداري في العديد من الدول كضمانة لحماية هذه الحقوق، حيث يسعى إلى فرض رقابته على مشروعية استخدام هذه التقنيات. وقد أسفر هذا الدور عن إصدار العديد من الأحكام والقرارات القضائية التي تشكل مرجعية حاسمة في تحديد الضوابط والمعايير القانونية لهذه الممارسات.

وفي هذا السياق، سنستعرض بعض التطبيقات القضائية لرقابة القضاء الإداري على المراقبة الرقمية في مختلف الأنظمة القانونية.

أولا: تطبيقات من الاجتهاد القضائي الفرنسي.

من بين أبرز الاجتهادات القضائية الحديثة التي تجسد تدخل القضاء الإداري لحماية الحقوق والحريات في سياق استخدام أدوات المراقبة الرقمية، القرار الصادر عن مجلس الدولة الفرنسي، بتاريخ 21 أبريل 2021، تحت رقم 393099. وقد نظر المجلس من خلال هذا القرار في طعن تقدمت به جمعيات حقوقية ضد استخدام وزارة الداخلية للطائرات المسييرة (drones) المزودة بكاميرات لتصوير التظاهرات والأماكن العامة، دون سند تشريعي خاص.

وقد اعتبر مجلس الدولة أن هذا الاستخدام يشكل مساساً بالحقوق في الخصوصية وحماية المعطيات الشخصية، وهو ما يخالف مبدأ المشروعية، خاصة في ظل غياب نص تشريعي يُؤطر بدقة شروط استعمال هذه الوسائل التكنولوجية. وأكد أن مجرد الغاية الأمنية لا تبرر المساس بالحريات، وأن أي تدخل من هذا النوع ينبغي أن يخضع لضوابط دقيقة تُحقق التناسب والضرورة، مع احترام الضمانات المنصوص عليها في القانون الفرنسي واللائحة الأوروبية العامة لحماية البيانات (GDPR).

وجاء في منطوق القرار منع الإدارة من مواصلة هذا النوع من المراقبة، إلى حين صدور تشريع يُحدد الإطار القانوني لها، مما يعكس دور القضاء الإداري الفرنسي في ضمان احترام الضوابط القانونية في المجال الرقمي، وتحقيق التوازن بين متطلبات الأمن العام وحماية الحقوق والحريات الأساسية، وفي مقدمتها الحق في الحياة الخاصة¹.

ثانياً: القضاء الإداري الألماني.

أصدرت المحكمة الإدارية العليا في ألمانيا (Bundesverwaltungsgericht) حكماً مهماً يتعلق باستخدام الكاميرات الذكية في الأماكن العامة، وذلك بتاريخ 27 مارس 2019. تناولت القضية تركيب طيبة أسنان في ولاية ببرندبورغ كاميرا رقمية فوق مكتب الاستقبال في عيادتها بهدف مراقبة الزوار، حيث كانت الصور تُعرض مباشرة على شاشات في غرف العلاج. اعترضت مفوضة حماية البيانات في الولاية على هذا الإجراء، مطالبة بتوجيه الكاميرا بحيث لا تُظهر المساحات العامة للعيادة. أيدت المحكمة قرار المفوضة، مشددة على أن أي استخدام للمراقبة بالفيديو في الأماكن العامة يجب أن يتوافق مع اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، ولا يجوز تطبيق القوانين الوطنية مثل "قانون تحسين المراقبة بالفيديو" إذا تعارضت مع أحكام الاتحاد الأوروبي. وقد أكدت المحكمة أن استخدام الكاميرات لا يكون مشروعاً إلا إذا كان ضرورياً لحماية مصالح مشروعة، وفقاً للمادة 6 من اللائحة، مثل منع الجرائم، ويستلزم ذلك إجراء تقييم دقيق لمدى الضرورة والملاءمة قبل الشروع في أي إجراء من هذا النوع. يُبرز هذا الحكم أهمية احترام الخصوصية الفردية وضرورة التوازن بين الأمن وحقوق المواطنين في القضاء العام².

ثالثاً: القضاء الإداري في جنوب أفريقيا.

في عام 2020، أصدرت المحكمة العليا في جنوب أفريقيا حكماً بارزاً في "قضية فومكام ضد وكالة الطرق الوطنية بجوهانسبرغ"، والتي نظرت في مشروعية استخدام تقنيات التعرف البصري في أنظمة المراقبة الأمنية بالأماكن العامة. وكانت شركة فومكام قد تقدمت بطلب لتركيب منظومة كاميرات ذكية مزودة بتقنيات التعرف

¹ Conseil d'État (Assemblée), 21 avril 2021, n°393099, Association Quadrature du Net et autres, publié au Recueil Lebon. Texte intégral disponible sur : <https://www.legifrance.gouv.fr>.

² Federal Administrative Court 27.03.2019. 6 C 2/18. Full text available on: <https://www.bverwg.de/en>

على الوجوه في الفضاء العام، إلا أن الوكالة رفضت الطلب استناداً إلى مخاوف مشروعة تتعلق بالخصوصية الفردية وإمكانية التوسع في المراقبة الجماعية، خاصة في ظل غياب إطار تشريعي واضح ينظم هذه الممارسات. غير أن المحكمة قضت بإجازة الطلب، بحجة أن قرار الرفض لم يستند إلى سند قانوني كاف، مع تأكيداً في الوقت ذاته على ضرورة خضوع أي تطبيق لهذه التقنيات لأحكام قانون حماية البيانات الشخصية. ويعد هذا الحكم تجسيدا عمليا للإشكاليات القانونية المترتبة على انتشار تقنيات المراقبة المتطورة، كما يسلط الضوء على الحاجة الماسة إلى وضع تشريعات شاملة توازن بين متطلبات الأمن الوطني وضمانات حماية الخصوصية الفردية¹.

رابعاً: القضاء الإداري في الهند.

في عام 2017، أصدرت المحكمة العليا في الهند حكماً تاريخياً في القضية المعروفة باسم K.S. Puttaswamy v. Union of India، اعتبر تحولاً جذرياً في حماية الخصوصية الرقمية. جاءت هذه الدعوى على خلفية الاعتراض على برنامج "آدهار" (Aadhaar)، وهو نظام الهوية البيومترية الوطني، بسبب ما يطرحه من تهديدات لخصوصية الأفراد نتيجة جمع وتخزين بياناتهم البيومترية والشخصية دون وجود إطار قانوني واضح ينظم هذه العملية. أصدرت هيئة المحكمة حكماً بالإجماع يقضي بأن الخصوصية حق دستوري جوهري، ورفضت أحكاماً سابقة كانت قد أنكرت وجود هذا الحق، مؤكدة أن أي تدخل حكومي في الخصوصية يجب أن يكون مستنداً إلى قانون واضح، ويحقق مصلحة مشروعة، ويكون متناسباً مع الهدف المرجو. أدى هذا الحكم إلى تحولات قانونية مهمة، أبرزها الدفع نحو سن قانون شامل لحماية البيانات الشخصية، وأصبح مرجعاً رئيسياً في قضايا الخصوصية والمراقبة الرقمية في الهند وخارجها².

خامساً: القضاء الإداري المصري.

في حكم تاريخي صادر عن المحكمة الإدارية العليا بتاريخ 15 أبريل 2017، ألغت المحكمة لائحة الجزاءات الصادرة عن وزير الاتصالات وتكنولوجيا المعلومات، والتي يوقعها الجهاز القومي لتنظيم الاتصالات على الجهات المرخص لها بالعمل في مجالات الاتصالات، لعدم عرضها على قسم التشريع بمجلس الدولة. وقد أكدت المحكمة في حيثيات حكمها أن عرض التشريعات واللوائح على قسم التشريع بمجلس الدولة هو إجراء وجوبي لتحقيق الأمان القانوني، وأن عدم عرضه يؤدي إلى بطلانها. وأشارت المحكمة إلى أن مراجعة التشريعات عمل فني لا يقدر عليه طبقاً للدستور إلا أهل الخبرة والتخصص من رجال مجلس الدولة، لتمتعهم

¹ Vumacam (Pty) Ltd v Johannesburg Roads Agency and Others (14867/20) [2020] ZAGPJHC 186 (20 August 2020). <https://www1.saflii.org/za/cases/ZAGPJHC/2020/186.html?utm>

² K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 – Supreme Court of India, Judgment dated 24 August 2017.

بالاستقلال عن السلطتين التنفيذية والتشريعية، لتجري المراجعة بحياد وتجرد بعيدا عن الضغوط أو الإملاءات أو غيرها من أمور قد تؤثر في سلامة إعداد مشروع التشريع¹.

الخاتمة:

من خلال ما سبق، يتضح أنه بقدر ما للمراقبة الرقمية من أهمية في حماية الأمن القومي للدول، فإنها في الوقت نفسه تشكل خطورة كبيرة على بعض أوجه حقوق الإنسان الأساسية، فيصبح تدخل القاضي الإداري أمراً ضرورياً باعتباره قاضي الحقوق والحريات الأساسية وحامي مبدأ المشروعية. وتوصلت الدراسة إلى النتائج التالية:

-القاضي الإداري قادر على حماية الحقوق في حالات واضحة الانتهاك (مثل تجاوز الصلاحيات)، لكنه عاجز عن مراقبة البرامج السرية أو غير المعلنة، مما يشكل حماية جزئية.
-الحماية القضائية أكثر فاعلية في الدول ذات الضمانات القوية مثل الاتحاد الأوروبي، بينما في بعض الأنظمة يكون دورها محدودا.

-رغم الجهود المبذولة من الهيئات الدولية والإقليمية ومختلف الدول من خلال العديد من التشريعات المتعلقة بتنظيم المراقبة الرقمية، إلا أن هذه النصوص أظهرت محدوديتها في مواجهة تقنيات حديثة ومتطورة.
-تعدد المواثيق الدولية بشأن تنظيم المراقبة الرقمية لا يجعل منها ضمانا لحماية الحقوق والحريات الأساسية للأفراد، لأنها غير ملزمة للدول ما لم تنص القوانين الداخلية على ذلك.

-بقدر ما للقاضي الإداري من سلطات بخصوص رقابة المراقبة الرقمية، إلا أنه قد يضيق نطاق الرقابة القضائية نتيجة مقتضيات حماية الأمن القومي أو في الظروف الاستثنائية.

-في بعض الأحيان يصعب على القاضي الإداري تقدير تعويض الأضرار الناجمة عن المراقبة الرقمية نتيجة الطبيعة المعقدة لتقنيات المراقبة من جهة، وسرية بعض الإجراءات المتخذة من جهة أخرى.
ومن التوصيات التي يمكن اقتراحها في هذا الإطار:

-ضرورة تكامل الحلول التقنية والقانونية والتنظيمية استجابة للمخاطر المتعددة التي تواجه حقوق الأفراد وحرياتهم في ظل المراقبة الرقمية.

-ضرورة تعزيز استقلالية القضاء، وإلزام الجهات الأمنية بالشفافية، وتدريب القضاة للتعرف على تقنيات المراقبة الحديثة وتزويدهم بالأدوات اللازمة لفحص المشروعية والتناسب.

¹ حكم المحكمة الإدارية العليا في الطعن رقم 29606 لسنة 62 قضائية عليا، بجلسة 2017/4/15، أثر عدم عرض لائحة الجزاءات الخاصة بالجهاز القومي لتنظيم الاتصالات على قسم التشريع بمجلس الدولة، وما متطلبات مبدأ الأمن القانوني.

- استشارة التقنيين المختصين عند سن التشريعات بما يضمن سلامتها واحتوائها لمختلف جوانب التأثيرات المحتملة لعملية المراقبة باستخدام التقنيات الرقمية الحديثة.
- ضرورة تحديث التشريعات الوطنية لمواكبة التطورات التكنولوجية وتوضيح إطار عمل استخدام المراقبة الإلكترونية، بما يضمن حماية الحقوق الأساسية للأفراد.
- تعزيز الرقابة القضائية من خلال توسيع سلطات القاضي الإداري في مراجعة قرارات استخدام التقنيات الإلكترونية والتأكد من التزام الأجهزة التنفيذية بالقوانين الوطنية والدولية.

قائمة المصادر والمراجع:

أولاً: النصوص القانونية.

- 1- المرسوم الرئاسي رقم 20-442 المؤرخ في 20 ديسمبر 2020 المتضمن التعديل الدستوري لسنة 2020، ج ر عدد 82 المؤرخة في 30 ديسمبر 2020.
- 2- القانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 14 الصادرة في 16 أوت 2009.
- 3- القانون رقم 18-07 المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، صادرة في 12 يونيو 2018.
- 4- المرسوم الرئاسي رقم 22-187 المؤرخ في 18 ماي 2022 يتضمن تعيين رئيس وأعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، جريدة رسمية عدد 34، الصادرة في 20 ماي 2022.
- 5- القانون رقم 94 لسنة 2015 المتعلق بمكافحة الإرهاب في مصر، الجريدة الرسمية العدد 33 مكرر الصادرة في 15 أوت 2015.
- 6- مرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية في الإمارات العربية، دخل حيز التنفيذ اعتباراً من 02 يناير 2022.
- 7- قانون حماية البيانات الفيدرالي الألماني الصادر في 30 يونيو 2017 (BGBI. I p. 2097) ، والذي تم تعديله آخر مرة بموجب المادة 7 من قانون 6 مايو 2024 (BGBI. 2024 I No. 149).

1-Electronic Communications Privacy Act of 1986, H.R.4952 — 99th Congress (1985-1986), The ECPA was significantly amended by the Communications Assistance to Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act in 2001, the USA PATRIOT reauthorization acts in 2006, and the FISA Amendments Act of 2008.

2- PL 103-359 H.R.4299 - Intelligence Authorization Act for Fiscal Year 1995, FISA has been significantly amended by the Intelligence Authorization Act of 1995

(Pub. L. 103-359; 10/14/94), by the Intelligence Authorization Act of 1999, (Pub. L. 105-272; 10/5/98), by the USA PATRIOT Act (Pub. L. 107-56; 10/26/01), by the USA PATRIOT Additional Reauthorization Amendments Act of 2006 (Pub. L. 109-178; (3/9/06), the FISA (Foreign Intelligence Surveillance Act) Amendments Act of 2008 (Pub. L.110-261; 7/10/2008).

3- LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF n°0235 du 8 octobre 2016.

4- Investigatory Powers Act 2016, UK Public General Acts 2016 c. 25.

ثانياً: الكتب

1- محمد رشاد الأمامي، القرار الإداري الإلكتروني وأوجه الرقابة عليه، دروب المعرفة للنشر والتوزيع، الإسكندرية، مصر، 2023.

2- مراد بدران، الرقابة القضائية على أعمال الإدارة العامة في ظل الظروف الاستثنائية (دراسة مقارنة)، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008.

3- خليل أحمد، القضاء الإداري وحماية الحريات الأساسية، دار الجامعة الجديدة، 2021.

4- علي دلشاد معروف، رقابة القضاء على مشروعية قرارات الضبط الإداري، الطبعة 0، مكتبة وفاء القانونية، الإسكندرية، مصر، 2016.

ثالثاً: الرسائل والمذكرات

1- بشير محمد حسين، أثر المراقبة الرقمية على الحريات العامة، رسالة ماجستير، في قانون الإدارة العامة، كلية الحقوق والعلوم السياسية، جامعة سيدي بلعباس، 2016-2017.

رابعاً: المقالات

1- العربي وردية، أساس الضرر الموجب للتعويض في مجال المسؤولية المدنية للدولة ودور القاضي الإداري في تقدير التعويض الخاص به، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 06، العدد 02، 2023.

2- زعزوعة فاطمة، أساس المسؤولية الإدارية عن أضرار المعالجة الآلية لمعطيات المرفق الإلكتروني، مجلة الدراسات القانونية والاقتصادية، المجلد 04، العدد 03، 2021.

خامساً: المواقع الإلكترونية

1- <https://arabi21.com/story/984298>

2- <https://www.techtarget.com/whatis/definition/Great-Firewall-of-China>

3- <https://www.un.org/ar/ga/77/resolutions.shtml>

4-<https://www.ohchr.org/ar/stories/2022/06/switching-internet-causes-incalculable-damage-un-report>

5-<https://www.ohchr.org/ar/documents/thematic-reports/ahrc5117-right-privacy-digital-age>

سادسا: المراجع الأجنبية

- 1- Dan Kaminski, La surveillance électronique des justiciables : légitimité publique et livraison privée ? Archives de politique criminelle 2013/1 (n° 35).
- 2- Dahmouche Faiza, The impact of the Fourth Industrial Revolution on the right to privacy, Jurisprudence Journal, Vol 61, (N°: 01- S N 33) Mars 2020.
- 3- Mark D. Young, ELECTRONIC SURVEILLANCE IN AN ERA OF MODERN TECHNOLOGY AND EVOLVING THREATS TO NATIONAL SECURITY, STANFORD LAW & POLICY REVIEW (vol22.1),2011.
- 4- Electronic Surveillance and Civil Liberties, Federal Government Information Technology: (Washington, DC: U.S. Congress, Office of Technology Assessment, OTACIT-293, October 1985).
- 5- Lenaerts, Koen. Digital Rights and Administrative Oversight, CMLR, Vol 58, 2021.
- 6- Mantelero, Alessandro, The Future of Data Protection: Digital Surveillance and Administrative Law, Springer, 2018.
- 7-Nolte, Georg, Federal Administrative Courts and Digital Surveillance in Germany, European Public Law, 2021.
- 8- Johan Wolswinkel, Intelligence artificielle et droit administratif, édition du conseil de l'Europe, décembre, 2022.