المنبر المصري
لحقوق الإنسان

تقرير

برمجة الصمت

كيف تُقيّد القوانين الحقوق الرقمية في مصر؟



المنبر المصري لحقوق الإنسان
Egyptian Human Rights Forum
Forum Egyptien pour les Droits de l'Homme

تجمع مستقل للمدافعين والمدافعات عن حقوق الإنسان المصريين الذين يجمعهم إيمان لا يتجزأ بالقيم العالمية لحقوق الإنسان، ورؤية عامة مشتركة لضرورة تأسيس نظام سياسي في مصر يقوم على احترام مبادئ حقوق الإنسان والديمقراطية والمواطنة. تأسس المنبر كمنظمة غير حكومية، ويضم في عضويته من المدافعين والمدافعات وبصفتهم الشخصية عددا عن حقوق الإنسان المنتمين لمجالات مهنية أ أكاديمية متنوعة، يسعى المنبر إلي التنسيق مع المنظمات الإقليمية والدولية المستقلة لحقوق الإنسان من أجل تعزيز الحماية الدولية لحقوق الإنسان.

Egyptianforum.org

@EgyptianHRforum

المحتويات

مقدمة	4
أولًا: الإطار الدستوري المتعلق بالحقوق والحريات الرقمية	7
ثانيًا: حجب المواقع والرقابة على المحتوى	11
ثالثًا: أزمة تراخيص المواقع الإلكترونية الصحفية في مصر	16
رابعًا: التوسع في تجريم وحيازة واستخدام معدات الاتصالات	20
خامسًا: المراقبة الجماعية	23
سادسًا: ضعف قواعد حماية البيانات الشخصية	27
سابعًا: جرائم نشر الأخبار الكاذبة والسبّ والقذف كأدوات ضبط رقمي	30
ثامنًا: السيطرة القانونية على منتجي المحتوى الرقمي عبر "إعادة التصنيف" و"التجريم الأخلاقي"	34
تاسعًا: مكافحة الإرهاب.. التشريع الذي يُحوّل الإنترنت إلى مساحة اشتباه دائمة	37
عاشرًا: العدالة الإجرائية في القضايا الرقمية	39
حادي عشر: القواعد المنظمة لقطع الاتصالات	44
ثاني عشر: تجريم التشفير وإخفاء الهوية	46
ثالث عشر: تجريم حيازة التقنيات المتطورة... الدرونز نموذجًا	48
التوصيات	52
الخاتمة	55

مقدمة

لا تُختبر الحقوق والحريات في المجال العام التقليدي وحده، إذ أن جزءًا متزايدًا من الحياة العامة انتقل إلى فضاء رقمي تتحكم فيه البنية التحتية للاتصالات، وسياسات المنصات، وقواعد البيانات، وآليات الترخيص والرقابة.ويتحول المساس بالحقوق والحريات في هذا الفضاء إلى تغيير في إمكانية ممارسة الحق أصلًا مثل إمكانية الوصول إلى المعلومات، وإمكانية النشر، وإمكانية التواصل الآمن، وإمكانية التنظيم والعمل الصحفي والبحثي دون خوف من الرصد أو العقاب.

لذلك فإن الحديث عن الحقوق الرقمية ليس حديثًا عن حقوق جديدة منفصلة، بقدر ما هو حديث عن الطريقة التي تُمارَس بها الحقوق والحريات في بيئة تقنية تجعل أثر القيد أسرع وأوسع وأقل قابلية للرصد المجتمعي مقارنةً بالقيود التقليدية.

يوفّر الدستور المصري إطارًا عامًا يمكن أن تُقرأ داخله الحقوق الرقمية بوصفها امتدادًا طبيعيًا لحرية الرأي والتعبير، وحرية الصحافة والإعلام، والحق في تداول المعلومات، وحرمة الحياة الخاصة وسرية المراسلات، وسيادة القانون والرقابة القضائية.

هذا الإطار الدستوري يضع الأصل لصالح الحماية، فحرية التعبير والإعلام تُقدَّم كقاعدة، وحظر الرقابة يُطرح كضمانة، وسرية الاتصالات تُحاط بقيود إجرائية واضحة، والحق في المعلومات يُفترض أن يكون قاعدة عامة، بينما يُفترض أن تبقى الاستثناءات محدودة ومحددة.

غير أن الإشكال العملي لا يبدأ عادةً من غياب النصوص الدستورية، بل من طريقة ترجمتها إلى تشريعات وإجراءات، ومن اتساع الاستثناءات وضعف الضمانات وغياب الشفافية الفعّالة. وبدلًا من أن يكون التنظيم القانوني أداة لتفعيل حماية الدستور، تتحول بعض القوانين واللوائح إلى مسارات تُعيد تعريف حدود الحق عبر معايير واسعة ومرنة مثل الأمن القومي والنظام العام والآداب العامة والقيم الأسرية.

وتتجلى إشكاليات الحقوق الرقمية في مصر في مسارات عدة أحدها هو مسار التحكم في المحتوى والنفاذ إليه، حيث يظهر الحجب وإجراءات الوقف والإزالة بوصفها أدوات عالية الأثر قد تُفعَّل عبر مداخل جنائية أو تنظيمية أو بنيوية متصلة بالبنية التحتية نفسها.

ومسار ثانٍ يربط الوجود الرقمي بشرط إداري سابق عبر منظومة تراخيص المواقع، بما يجعل استمرار المنصات الصحفية المستقلة أو المبادرات الرقمية مرتبطًا بقرار إداري قابل للتعطيل أو السحب، ويجعل التدخل يقع أولًا ثم يُراجع لاحقًا.

ومسار ثالث يتصل بتوسيع التجريم الجنائي في قضايا النشر، عبر نصوص مرنة يمكن إسقاطها بسهولة على التعبير عبر الإنترنت، بحيث تتحول المنطقة الفاصلة بين الرأي والمعلومة والخطأ المهني إلى منطقة اتهام محتملة.

ومسار رابع يتعلق ببناء قدرات مراقبة دائمة من خلال تمكين فني داخل الشبكات، والاحتفاظ الإلزامي بالبيانات، وتوسيع سلطات الاعتراض، بما يجعل جمع البيانات قاعدة تشغيل ثم يصبح الفحص قرارًا لاحقًا، وهو ترتيب يضاعف مخاطر التعسف لأنه يحول المجتمع كله إلى مخزون بيانات جاهز للاستخدام.



شكل (1): المسارات الأربعة لتقييد الفضاء الرقمي

ومع هذه المسارات تظهر إشكالية الضمانات بوصفها الفارق بين تنظيم مشروع وبين قيد يهدم جوهر الحق. فوجود إجراء من نوع عرض القرار على جهة قضائية أو تسبيب مكتوب لا يكفي إذا كانت المعايير التي يقوم عليها التدخل فضفاضة، أو إذا كانت الرقابة متأخرة، أو إذا كانت قدرة الطعن بطيئة مقارنةً بأثر القرار، أو إذا كان التنفيذ الفوري يقع على عاتق مقدمي الخدمة بما يدفعهم إلى توسيع نطاق الحجب والامتثال خوفًا من المسؤولية.

كما أن ضعف الشفافية يجعل المجتمع عاجزًا عن تقييم حجم التدخل ومعاييره وأخطائه، ويجعل معرفة من المسؤول عن القرار وكيف يُراجع قرارًا صعبة، وهو ما يضعف عمليًا الحق في الانتصاف الفعّال.

ومن زاوية أخرى، يضيف تنظيم التكنولوجيا ذاتها طبقة جديدة من المخاطر. فعندما تُعامل أدوات الحماية الرقمية مثل التشفير أو أدوات الاتصال أو التقنيات المتقدمة بوصفها قدرة مشروطة بإذن مسبق، يصبح الحق الوقائي نفسه قابلاً للتعليق. وبالتالي لا يدور النقاش حول تجريم فعل ضار محدد، بل حول تجريم سابق على الفعل يطال الحيازة أو الاستخدام أو البحث والتجريب، ويجعل المجال التقني والبحثي والاقتصادي يعمل تحت تهديد عدم اليقين.

وذلك ما يجعل الامتثال مهمة شاقة، وتصبح الانتقائية في الإنفاذ احتمالًا قائمًا، وتصبح كلفة الابتكار أعلى، خصوصًا على الفاعلين الصغار والباحثين والمبادرات المستقلة.

انطلاقًا من هذا، يتناول هذا التقرير، «برمجة الصمت: كيف تُقيّد القوانين الحقوق الرقمية في مصر؟»، بنية التنظيم القانوني للفضاء الرقمي في مصر من زاوية حقوقية، بهدف فهم منطقها وآثارها على حدود الحقوق وضماناتها. ويعمل على بيان الكيفية التي يُعاد بها توزيع العلاقة بين الأصل والاستثناء في التشريعات والممارسات، وكيف تتراجع قابلية التوقع القانوني، وكيف ينعكس ذلك على حرية التعبير والعمل الصحفي والبحثي والتقني، وعلى الحق في الخصوصية والحق في المعرفة.

كما يرصد التقرير تشكل بيئة قانونية تُنتج أثرًا ردعيًا يدفع إلى رقابة ذاتية ويقلص مساحة المشاركة العامة حتى قبل الوصول إلى الإدانة. ويقوم في تحليله على اختبار العناصر الحاكمة لأي تدخل يمس الحقوق الرقمية، وهي وضوح القاعدة القانونية، وضيق

معيار التدخل، وضرورة الإجراء وتناسبه، وفعالية الرقابة القضائية، وتوافر مسارات طعن سريعة ومفهومة، ودرجة شفافية تمنع التعسف وتتيح المراجعة العامة.



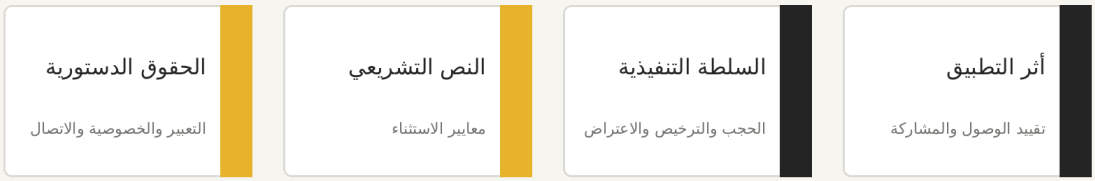
شكل (2): العناصر الحاكمة لاختبار مشروعية أي تدخل

وبناءً على ذلك، يسعى التقرير إلى طرح توصيات لإعادة التوازن بين مقتضيات الحماية وبين جوهر الحقوق والحريات وضماناتها الإجرائية. وذلك بهدف ضبط دور الدولة حتى لا يتحول إلى إدارة عامة للمجال الرقمي بمنطق الاشتباه الدائم. فالأمن الحقيقي في الفضاء الرقمي لا يتحقق بزيادة نطاق التدخل، بل ببناء قواعد واضحة يمكن توقعها، وبضمانات رقابية مستقلة، وبسياسات تشجع أمن الاتصالات وحماية البيانات، وبمنظومة قانونية تمنع أن يصبح الإنترنت مساحة قابلة للتعليق كلما اتسع التفسير أو غابت الحدود.

> **«الأمن الحقيقي في الفضاء الرقمي لا يتحقق بزيادة نطاق التدخل، بل ببناء قواعد واضحة يمكن توقعها»**

أولًا: الإطار الدستوري المتعلق بالحقوق والحريات الرقمية

من الضمانة الدستورية إلى قيد الممارسة



يضع الدستور المصري الصادر عام 2014 (بتعديلاته) أساسًا يمكن قراءة الحقوق الرقمية في إطاره، بوصفها امتدادًا لحقوق وحريات تقليدية (حرية التعبير، حرية الإعلام، الحق في الخصوصية، حرية تداول المعلومات، ضمانات سيادة القانون) تعمل اليوم داخل فضاء رقمي/معلوماتي تتداخل فيه وسائل النشر والاتصال والبنية التحتية للاتصالات مع ممارسة الحقوق ذاتها.

على مستوى حرية التعبير، تنص المادة (65) من الدستور[1] على كفالة حرية الفكر والرأي، وعلى حق كل إنسان في التعبير عن رأيه "بالقول، أو بالكتابة، أو بالتصوير، أو غير ذلك من وسائل التعبير والنشر"، وهي صياغة تستوعب بطبيعتها وسائط التعبير الرقمية المختلفة (منشورات المنصات، الفيديو، البودكاست، التدوين، الرسائل العامة...) دون حاجة إلى إضافة دستورية خاصة بالإنترنت.

ويكتمل هذا الإطار في مجال الإعلام والنشر بالمادتين (70) و(71) من الدستور. فالمادة (70)[2] تقرر حرية الصحافة والطباعة والنشر بأشكاله الورقية والمرئية والمسموعة والإلكترونية، كما تقرر حق إنشاء وسائل الإعلام ووسائط الإعلام الرقمي، مع إحالة بعض الاجراءات التفصيلية إلى القانون (مثل إجراءات إنشاء وتملك محطات البث والصحف الإلكترونية).

أما المادة (71)[3] فترسي ضمانة جوهرية بحظر فرض الرقابة أو المصادرة أو الوقف أو الإغلاق على الصحف ووسائل الإعلام، ولا تجيز الاستثناء إلا "زمن الحرب أو التعبئة العامة" وبحدود رقابة محددة، وتضيف قيدًا مهمًا على العقوبات السالبة للحرية في جرائم النشر مع استثناءات بعينها (كالتحريض على العنف أو التمييز أو الطعن في الأعراض). هذا المزيج يُنتِج، داخل الدستور نفسه، توازنًا بين أصل الحماية (المنع والحظر) وبين استثناءات منصوص عليها صراحة.

[1] مادة (65): حرية الفكر والرأى مكفولة. ولكل إنسان حق التعبيرعن رأيه بالقول، أو بالكتابة، أو بالتصوير، أو غير ذلك من وسائل التعبير والنشر.

[2] مادة (70): حرية الصحافة والطباعة والنشر الورقى والمرئى والمسموع والإلكترونى مكفولة، وللمصريين من أشخاص طبيعية أو اعتبارية، عامة أو خاصة، حق ملكية وإصدار الصحف وإنشاء وسائل الإعلام المرئية والمسموعة، ووسائط الإعلام الرقمى. وتصدر الصحف بمجرد الإخطار على النحو الذى ينظمه القانون. وينظم القانون إجراءات إنشاء وتملك محطات البث الإذاعى والمرئى والصحف الإلكترونية.

[3] مادة (71): يحظر بأى وجه فرض رقابة على الصحف ووسائل الاعلام المصرية أو مصادرتها أو وقفها أو إغلاقها. ويجوز استثناء فرض رقابة محددة عليها فى زمن الحرب أو التعبئة العامة. ولا توقع عقوبة سالبة للحرية فى الجرائم التى ترتكب بطريق النشر أو العلانية، أما الجرائم المتعلقة بالتحريض على العنف أو بالتمييز بين المواطنين أو بالطعن في أعراض الأفراد، فيحدد عقوباتها القانون.

ويقر الدستور كذلك الحق في المعلومات بوصفها قاعدة عامة وبالتالي تنطبق على الفضاء الرقمي. فالمادة (68)[4] تقرر أن المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، وأن الإفصاح عنها حق تكفله الدولة لكل مواطن، مع التزامها بتوفيرها وإتاحتها بشفافية، وإحالة تنظيم ضوابط الحصول عليها وسريتها وطرق التظلم والعقوبات على حجبها إلى القانون. وهذه المادة تكتسب أهمية في السياق الرقمي لأنها تشير صراحة إلى التزام مؤسسات الدولة بحفظ الوثائق الرسمية ورقمنتها "بجميع الوسائل والأدوات الحديثة"، بما يفتح -من زاوية دستورية- بابًا لقراءة الحكومة الرقمية والأرشفة الرقمية والبيانات المفتوحة كجزء من بنية الحق في الحصول على المعلومات وتداولها.

وفي محور الخصوصية وسرية الاتصالات، تقرر المادة (57)[5] حرمة الحياة الخاصة، وتقرر حرمة وسرية المراسلات بمختلف صورها، بما فيها المراسلات والاتصالات الإلكترونية، وتحظر مصادرتها أو الاطلاع عليها أو رقابتها إلا "بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون". وبالتالي يضع الدستور ضمانات إجرائية دقيقة تتمثل في اشتراط الأمر القضائي والتسبيب والتحديد الزمني، وقصر التدخل على "أحوال" مُحدّدة ينبغي تحديدها بالقانون. وتتضمن المادة (57) كذلك ضمانة دستورية تتجاوز حماية السرية إلى حماية "إتاحة الاتصال" ذاتها؛ إذ تُلزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، وتحظر تعطيلها أو وقفها أو حرمان المواطنين منها على نحو تعسفي، مع إحالة تنظيم ذلك إلى القانون.

وأهمية هذا أنه يؤسس لالتزام إيجابي على الدولة لا يقتصر على الامتناع عن التدخل في الاتصالات، بل يفرض واجبًا بحماية إمكانية النفاذ إلى خدمات الاتصال واستمراريتها بوصفها شرطًا لممارسة حقوق أخرى في الفضاء الرقمي (مثل التعبير وتلقي المعلومات والعمل الصحفي والتنظيم). وفي الوقت نفسه، فإن إحالة تنظيم ذلك إلى القانون تقتضي-من منظور دستوري- أن يظل أي تقييد محكومًا بضوابط الضرورة والتناسب وقابلية التوقع، وألا يتحول التنظيم إلى قناة تُمكّن من قطع الخدمة أو تقييدها بغير ضمانات.

وإلى جانب ذلك، يعزز الدستور منطق الحماية الإجرائية عبر مواد "سيادة القانون" والضمانات القضائية العامة؛ فالمادة (94)[6] تقرر أن سيادة القانون أساس الحكم، وأن خضوع الدولة للقانون واستقلال القضاء ضمانات أساسية لحماية الحقوق والحريات. كما تقرر المادة (95) [7]مبدأ الشرعية الجنائية (لا جريمة ولا عقوبة إلا بناء على قانون، ولا توقع عقوبة إلا بحكم قضائي)، وتقرر المادة (97)[8] حظر تحصين أي عمل أو قرار إداري من رقابة القضاء. وتضيف المادة (99)[9] وصف الاعتداء على الحرية الشخصية أو حرمة الحياة الخاصة وغيرها من الحقوق والحريات بأنه جريمة لا تسقط بالتقادم مع تقرير حق المضرور في اللجوء للقضاء.

---

[4] مادة (68): المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمدًا. وتلتزم مؤسسات الدولة بإيداع الوثائق الرسمية بعد الانتهاء من فترة العمل بها بدار الوثائق القومية، وحمايتها وتأمينها من الضياع أو التلف، وترميمها ورقمنتها، بجميع الوسائل والأدوات الحديثة، وفقاً للقانون.

[5] مادة (57): للحياة الخاصة حرمة، وهى مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائى مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين فى استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفى، وينظم القانون ذلك.

[6] المادة (94): سيادة القانون أساس الحكم في الدولة. وتخضع الدولة للقانون، واستقلال القضاء، وحصانته، وحيدته، ضمانات أساسية لحماية الحقوق والحريات.

[7] المادة (95): العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناء على قانون، ولا توقع عقوبة إلا بحكم قضائى، ولا عقاب إلا على الأفعال اللاحقة لتاريخ نفاذ القانون.

[8] المادة (97): التقاضى حق مصون ومكفول للكافة. وتلتزم الدولة بتقريب جهات التقاضى، وتعمل على سرعة الفصل في القضايا، ويحظر تحصين أى عمل أو قرار إدارى من رقابة القضاء، ولا يحاكم شخص إلا أمام قاضيه الطبيعى، والمحاكم الاستثنائية محظورة.

[9] المادة (99): كل اعتداء على الحرية الشخصية أو حرمة الحياة الخاصة للمواطنين، وغيرها من الحقوق والحريات العامة التي يكفلها الدستور والقانون، جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم،وللمضرور إقامة الدعوى الجنائية بالطريق المباشر. وتكفل الدولة تعويضا عادلا لمن وقع عليه الاعتداء، وللمجلس القومى لحقوق الإنسان إبلاغ النيابة عن أى انتهاك لهذه الحقوق، وله أن يتدخل في الدعوى المدنية منضماً إلي المضرور بناء على طلبه، وذلك كله على الوجه المبين بالقانون.

وهذه المنظومة، وإن لم تُكتب خصيصًا للفضاء الرقمي، فإنها تمنح الأثر الرقمي للحقوق (المراقبة، النفاذ إلى البيانات، القيود الإدارية على المحتوى أو الاتصال) إطارًا دستوريًا يربط القيود بمشروعية القانون وبالرقابة القضائية.

كما تعامل الدستور مع مفهوم أمن الفضاء المعلوماتي؛ فالمادة (31)[10] تعتبر أمن الفضاء المعلوماتي جزءًا أساسيًا من منظومة الاقتصاد والأمن القومي، وتُلزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه "على النحو الذي ينظمه القانون". أهمية هذه المادة أنها تُدخل الأمن السيبراني إلى مستوى دستوري، إلا أنها في الوقت نفسه تعتمد تقنية الإحالة التشريعية، ما يجعل تعريف الخطر ومعايير التدابير وحدودها مسألة حاسمة في كيفية ترجمة هذا الالتزام إلى قواعد قابلة للتوقع.

ويضيف الدستور طبقة حماية مهمة عبر المادة (92) [11]تقرر قاعدة حاكمة مفادها أن الحقوق والحريات اللصيقة بشخص المواطن لا تقبل تعطيلًا ولا انتقاصًا، وأنه لا يجوز لأي قانون ينظم ممارسة الحقوق والحريات أن يقيدها بما يمس أصلها وجوهرها. كما ان المادة (93) [12]تمنح الاتفاقيات والعهود والمواثيق الدولية لحقوق الانسان التي تصدق عليها مصر قوة القانون بعد نشرها. ومن أبرز هذه الصكوك العهد الدولي الخاص بالحقوق المدنية والسياسية والذي صدّقت عليه مصر سنة 1982؛ وتكفل المادة (19)[13] من العهد حرية التعبير بما يشمل التماس المعلومات وتلقيها ونقلها بكل الوسائل، ولا تُجيز تقييدها إلا بقيود ينص عليها القانون وتكون ضرورية لاحترام حقوق الآخرين أو لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة، بينما تحظر المادة (17)[14] من ذات العهد أي تدخل تعسفي أو غير قانوني في خصوصية الفرد أو مراسلاته. وبناءً على ذلك فإن أي تشريع أو إجراء يفرض قيوداً على الحقوق الرقمية دون أن يستوفي شروط المشروعية والضرورة والتناسب لا يتوقف على كونه مخالفة دستورية بل يعد إخلالاً بالتزام دولي لمصر.

ورغم أن الدستور يرسم تصورًا يقوم على حماية حرية التعبير والإعلام بوصفها أصلًا، وعلى حظر الرقابة كقاعدة، وعلى أن أي مساس بسرية الاتصالات أو تعطيل لوسائل الاتصال العامة يجب أن يظل استثناءً مقيدًا بضمانات إجرائية وحدود زمنية ورقابة قضائية فعّالة، فإن جزءًا من التشريع اللاحق تعامل مع المجال الرقمي بمنطق التحكم السلطوي وليس بضمانة الحقوق.

يتجلى ذلك في نقل مركز الثقل من قواعد واضحة قابلة للتوقع إلى معايير مرنة مثل الأمن القومي والنظام العام والآداب العامة والقيم الأسرية، بما يجعل نطاق القيد قابلًا للتمدد بحسب التفسير لا بحسب ضابط موضوعي ثابت. كما يظهر في تحويل التنظيم

10 المادة(31): أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون.

11 المادة(92): الحقوق والحريات اللصيقة بشخص المواطن لا تقبل تعطيلاً ولا انتقاصًا. ولا يجوز لأى قانون ينظم ممارسة الحقوق والحريات أن يقيدها بما يمس أصلها وجوهرها.

12 المادة(93): تلتزم الدولة بالاتفاقيات والعهود والمواثيق الدولية لحقوق الإنسان التي تصدق عليها مصر، وتصبح لها قوة القانون بعد نشرها وفقاً للأوضاع المقررة.

13 المادة 19 : (i) لكل إنسان حق في اعتناق آراء دون مضايقة.

(ii) لكل إنسان حق في حرية التعبير. ويشمل هذا الحق حريته في التماس مختلف ضروب المعلومات والأفكار وتلقيها ونقلها إلى آخرين دونما اعتبار للحدود، سواء على شكل مكتوب أو مطبوع أو في قالب فني أو بأية وسيلة أخرى يختارها.

(iii) تستتبع ممارسة الحقوق المنصوص عليها في الفقرة 2 من هذه المادة واجبات ومسئوليات خاصة. وعلى ذلك يجوز إخضاعها لبعض القيود ولكن شريطة أن تكون محددة بنص القانون وأن تكون ضرورية :

(أ) لاحترام حقوق الآخرين أو سمعتهم،

(ب) لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

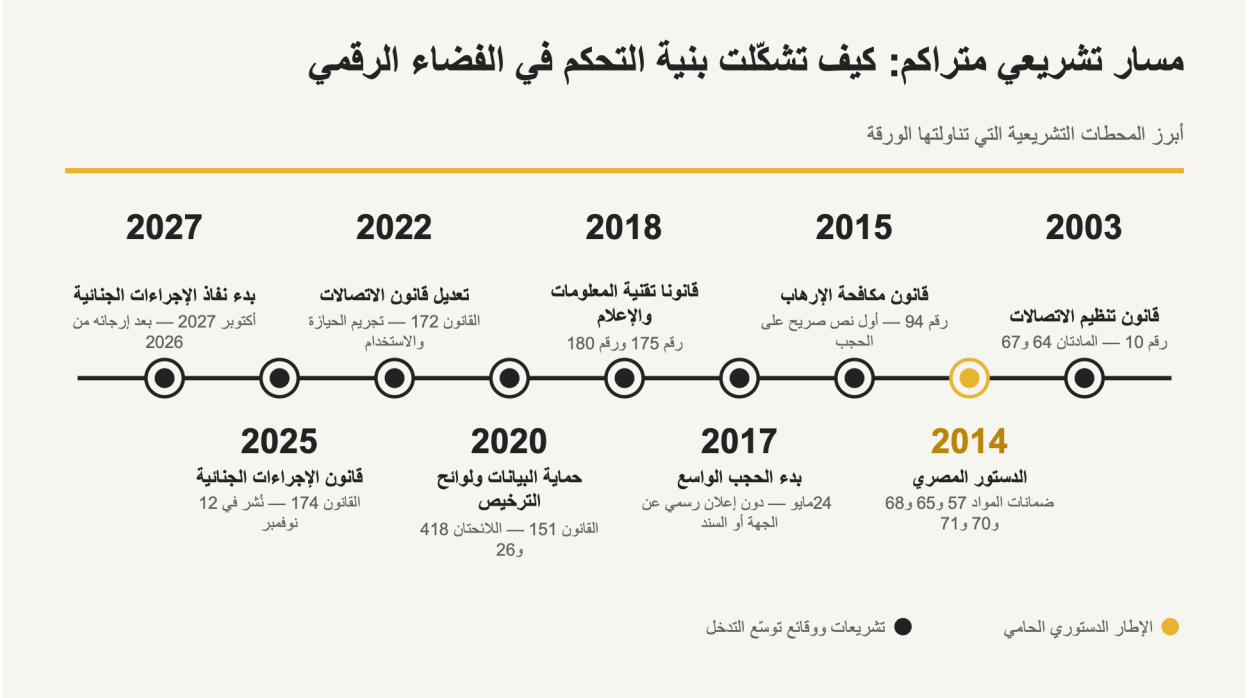
14 المادة 17 (i) لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.

(ii) من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس.

القانوني إلى مسار يتيح إجراءات سريعة عالية الأثر تمس إتاحة المحتوى أو النفاذ إليه (مثل الحجب أو الإزالة أو وقف الحسابات) دون أن تمر دائمًا بسلم ضمانات مكافئ لخطورة الأثر، وبما يطابق "الرقابة" حتى إن لم تُسمّ رقابة.

وعلى مستوى الخصوصية، بنت القوانين ترتيبات تجعل جمع البيانات والاحتفاظ بها وإتاحتها عند الطلب جزءًا من التشغيل المعتاد، بما يضعف عمليًا فلسفة الدستور التي تفترض أن التدخل في الاتصالات محدد ومسبب ومؤقت. وإلى جانب ذلك، أدخلت القوانين منطق الترخيص/الموافقة المسبقة في مجالات تمس أدوات الحماية الرقمية نفسها (كتقنيات التشفير أو بعض معدات الاتصال)، وهو ما يعيد توصيف الحق الوقائي كقدرة مشروطة، ويزيد أثر الردع والامتثال الذاتي.

وبالتالي فإن هذه القوانين تُمثّل انزياحًا في الوظيفة من قانون يُفترض أن يفعّل ضمانات الدستور إلى قانون يُعيد تعريف حدود الحق عبر بوابات واسعة تُضعف جوهر الحماية الدستورية. وقد ظهر ذلك في قانون تنظيم الإعلام والصحافة، وقانون مكافحة الإرهاب، وقانون مكافحة جرائم تقنية المعلومات، وقانون حماية البيانات الشخصية، بالإضافة إلى قانون تنظيم الاتصالات وتعديلاته.



شكل (3): المحطات التشريعية الرئيسية 2003–2026

ثانيًا: حجب المواقع والرقابة على المحتوى



مساحة المشاركة العامة أمام أدوات الحجب والترخيص

منذ 24 مايو 2017 بدأ الحجب كممارسة على نطاق واسع دون إعلان رسمي عن الجهة التي أصدرت القرار أو الأساس القانوني الدقيق، ثم اتسع الحجب تدريجيًا ليشمل منصات سياسية وحقوقية وخدمات تقنية وأدوات تجاوز الحجب[15].

يُفهم الحجب في السياق المصري بوصفه مجموعة تدابير قانونية إدارية وقضائية تُفضي عمليًا إلى منع وصول المستخدم إلى موقع أو رابط أو محتوى أو حساب، أو تعطيل أو إيقاف بث مادة إعلامية، أو إخضاع شبكات وخدمات الاتصالات لإدارة السلطات بما يسمح بالتحكم في النفاذ أو الاستمرارية. والتنظيم القانوني للحجب له قواعد متشعبة لا يَرِد في قانون واحد على سبيل الحصر، بل يتوزع بين قوانين تتعامل مع المحتوى وقوانين تتعامل مع البنية التحتية للاتصالات وقوانين توسّع أدوات التدخل باسم مكافحة الإرهاب.

ففي قانون مكافحة الإرهاب رقم 94 لسنة 2015 وهو أول قانون يتحدث عن إجراء الحجب صراحة، يظهر الحجب باعتباره إجراءً مرتبط بتجريم استخدام الشبكات لأغراض إرهابية. إذ تُجرِّم(المادة 29)[16] من القانون إنشاء أو استخدام موقع على شبكات الاتصالات أو شبكة المعلومات الدولية بقصد الترويج لأفكار داعية لارتكاب أعمال إرهابية أو لتضليل السلطات الأمنية أو للتأثير على سير العدالة أو لتبادل الرسائل والتكليفات بين الجماعات الإرهابية أو نقل معلومات عن تحركات الإرهابيين.

[15] حجب مواقع الوِب في مصر "التكنيكات والقوانين"، مؤسسة مسار، مايو 20241، الرابط: https://bit.ly/3OEiJmU

[16] المادة 29 يُعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعاً على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعاً إلكترونياً تابعاً لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها.

ثم تمنح (المادة 49)[17] من القانون للنيابة العامة أو سلطة التحقيق المختصة (بحسب الأحوال) سلطة اتخاذ بعض التدابير ضد المواقع الإلكترونية، إذ تنص على أن للنيابة أو سلطة التحقيق وقف المواقع المشار إليها بالفقرة الأولى من (المادة 29) أو حجبها، أو حجب ما يتضمنه أي وجه من أوجه الاستخدام مع التحفظ على الأجهزة والمعدات المستخدمة في الجريمة؛ وهو ما يعني أن الحجب هنا يُطرح كأداة لضبط أثر الجريمة أو منع استمرارها.

أما قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، فيتخذ فيه الحجب مسارًا إجرائيًا أكثر تفصيلاً. فالمادة 7[18] من القانون تُجيز لجهة التحقيق المختصة أن تأمر بحجب الموقع متى قامت أدلة على أن موقعًا يبث داخل الدولة أو خارجها يضع موادّ تُعد جريمة من الجرائم المنصوص عليها بالقانون وتشكل تهديدًا للأمن القومي أو تُعرِّض أمن البلاد أو اقتصادها القومي للخطر.

وتُلزم المادة جهة التحقيق بعرض أمر الحجب على المحكمة المختصة منعقدة في غرفة المشورة خلال 24 ساعة مشفوعًا بمذكرة بالرأي، وتصدر المحكمة قرارًا مسببًا خلال مدة لا تجاوز 72 ساعة بالقبول أو الرفض.

كما يضع القانون آلية عاجلة تُتيح لجهات التحري والضبط (الجهات الشرطية) عند الاستعجال لوجود خطر حال أو ضرر وشيك إبلاغ الجهاز القومي لتنظيم الاتصالات لإخطار مقدم الخدمة بالحجب المؤقت فورًا، على أن يُعرض محضر الإجراءات على جهة التحقيق خلال 48 ساعة وإلا عُدّ الحجب كأن لم يكن، مع إمكان إنهاء الحجب أو تعديل نطاقه أثناء نظر الدعوى بناء على طلب جهة التحقيق أو الجهاز أو ذوي الشأن.

[17] المادة 49: للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في الجرائم المنصوص عليها بالمواد (12، 15، 19، 22) من هذا القانون، أن تصدر أمراً مؤقتاً بغلق المقار، والأماكن، والمساكن، ومحال الإيواء على أن يصدر القرار من رئيس نيابة على الأقل، وتعتبر الأمتعة والأثاث المضبوط فيها في حكم الأشياء المحجوز عليها إدارياً بمجرد ضبطها حتى يفصل في الدعوى نهائياً، وتسلم بعد جردها وإثباتها في محضر إلى حارس يكلف بحراسة الأختام الموضوعة على المقر أو المكان أو المحل أو المسكن المغلق، فإن لم توجد مضبوطات كلف بالحراسة على الأختام وبالطريقة ذاتها، ويترتب على صدور الحكم بالبراءة سقوط أمر الغلق.
وللنيابة العامة أو سلطة التحقيق المختصة وقف المواقع المنصوص عليها في الفقرة الأولى من المادة (29) من هذا القانون، أو حجبها، أو حجب ما يتضمنه أي وجه من أوجه الاستخدام المنصوص عليها في هذه المادة، والتحفظ على الأجهزة والمعدات المستخدمة في الجريمة.

[18] المادة (7) الإجراءات والقرارات الصادرة بشأن حجب المواقع:
لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أى عبارات أو أرقام أو صور أو أفلام أو أية م مواد دعائية، أو ما فى حكمها مما يعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدا للأمن القومى أو تعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيا.
وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة فى غرفة المشورة، خلال 24 ساعة، مشفوعا بمذكرة برأيها، وتصدر المحكمة قرارها فى الأمر مسببا، فى مدة لا تجاوز 72 ساعة من وقت عرضه عليها، بالقبول أو بالرفض.
ويجوز فى حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع من ارتكاب جريمة، أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز – (فى إشارة للجهاز القومى لتنظيم الاتصالات) – ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المواقع أو الروابط أو المحتوى المذكور فى الفقرة الأولى من هذه المادة وفقا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.
وعلى جهة التحرى والضبط المُبلغة أن تعرض محضرا تثبت فيه ما تم من إجراءات على جهة التحقيق المختصة، وذلك خلال 48 ساعة من تاريخ الإبلاغ الذى وجهته للجهاز، وتتبع فى هذا المحضر ذات الإجراءات المبينه بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها فى هذه الحالة، أما بتأييد ما تم من إجراءات حجب أو بوقفها. فإذا لم يعرض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد، يعد الحجب الذى تم كأن لم يكن.
ولمحكمة الموضوع أثناء نظر الدعوى أو بناء على طلب جهة التحقيق أو الجهاز أو ذوى الشأن – أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه.
وفى جميع الأحوال يسقط القرار الصادر بالحجب بصدور أمر بأن لا وجه لإقامة الدعوى الجنائية أو بصدور حكم نهائى فيها بالبراءة".



شكل (4): المساران الزمنيان للحجب وفق المادة 7 من قانون تقنية المعلومات

من جهة أخرى يأتي قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام رقم 180 لسنة 2018 ليؤطر الحجب بوصفه أداة تنظيمية ورقابية على المحتوى والوسائل الصحفية والإعلامية والمواقع والحسابات المؤثرة التي يتجاوز عدد متابعيها 5 الاف متابع.

تقرر (المادة 3)[19] من القانون مبدأ حظر فرض الرقابة على الصحف ووسائل الإعلام أو مصادرتها أو وقفها أو إغلاقها، لكنها تفتح استثناءً "في زمن الحرب أو التعبئة العامة" لفرض رقابة محددة؛ وفي هذه الحالة تُجيز للمجلس الأعلى لتنظيم الإعلام أن يصدر قرارًا بضبط نسخ الصحيفة الورقية أو "حذف أو حجب المادة المخالفة" إذا نُشرت في صحيفة إلكترونية أو موقع إلكتروني أو وقف إعادة بثها، مع النص على حق ذوي الشأن في الطعن على قرار الحجب أمام محكمة القضاء الإداري.

ومن ناحية ثانية، تربط (المادة 6)[20] من القانون بين حصول الموقع على ترخيص من المجلس الأعلى لتنظيم الإعلام وبين استمرار النشاط الرقمي: فلا يجوز تأسيس مواقع إلكترونية أو إدارتها داخل مصر أو إدارة مكاتب أو فروع لمواقع تعمل من خارجها إلا بعد الحصول على ترخيص من المجلس الأعلى، وللمجلس في حالة مخالفة ذلك اتخاذ إجراءات -بما في ذلك- إلغاء الترخيص أو وقف النشاط أو حجب الموقع عند عدم الحصول على ترخيص سارٍ.

---

[19] مادة (3):
يحظر، بأي وجه، فرض رقابة على الصحف ووسائل الإعلام المصرية، ويحظر مصادرتها، أو وقفها، أو إغلاقها.
ويجوز استثناء فرض رقابة محددة عليها في زمن الحرب أو التعبئة العامة.
وفي هذه الحالة للمجلس الأعلى أن يصدر قرارا بضبط نسخ الصحيفة الورقية أو حذف أو حجب المادة المخالفة لتعليمات الرقابة في حالة نشرها في صحيفة إلكترونية أو موقع إلكتروني، أو وقف إعادة بثها في الوسيلة الإعلامية، ولذوي الشأن الطعن على القرار الصادر بذلك أمام محكمة القضاء الإداري.

[20] مادة (6): لا يجوز تأسيس مواقع إلكترونية في جمهورية مصر العربية، أو إدارتها، أو إدارة مكاتب أو فروع لمواقع إلكترونية تعمل من خارج الجمهورية، إلا بعد الحصول على ترخيص بذلك من المجلس الأعلى وفق الضوابط والشروط التي يضعها في هذا الشأن.
ومع عدم الإخلال بالعقوبات الجنائية المقررة، للمجلس الأعلى في حالة مخالفة أحكام الفقرة السابقة اتخاذ الإجراءات اللازمة بما في ذلك إلغاء الترخيص، أو وقف نشاط الموقع أو حجبه، في حالة عدم الحصول على ترخيص سار.
ولذوي الشأن الطعن على القرار الصادر بذلك أمام محكمة القضاء الإداري.

كما توسّع (المادة 19)[21] من القانون نطاق التدخل في عمل المواقع والمدونات والحسابات الشخصية إذا بلغ عدد متابعيها خمسة آلاف متابع أو أكثر، إذ تحظر نشر أو بث أخبار كاذبة أو التحريض على مخالفة القانون أو العنف أو الكراهية أو التمييز أو الطعن في الأعراض أو السب أو القذف أو امتهان الأديان، وتُلزم المجلس الأعلى باتخاذ الإجراء المناسب، وللمجلس الأعلى في سبيل مواجهة تلك المخالفات وقف أو حجب الموقع أو المدونة أو الحساب بقرار منه.

أما قانون تنظيم الاتصالات رقم 10 لسنة 2003، فلا يَرِد به الحجب كمصطلح قانوني واضح ومباشر، لكن نصوص القانون تعطي أدوات تمكين الدولة من التحكم في الشبكات والخدمات بما يمكن أن ينعكس على النفاذ فعليًا عند تفعيلها. فالمادة 64 تُلزم مشغلي ومقدمي خدمات الاتصالات بعدم استخدام أجهزة لتشفير خدمات الاتصالات إلا بعد موافقة الجهاز والقوات المسلحة وأجهزة الأمن القومي، كما تُلزم المشغل/مقدم الخدمة بتوفير الإمكانيات الفنية داخل الشبكة بما يتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها "في حدود القانون" مع مراعاة حرمة الحياة الخاصة.

والنص الأكثر اتصالًا بعملية الحجب أو بإمكانات التعطيل ومنع النفاذ هو نص المادة 67 التي تجيز للسلطات المختصة في الدولة أن تُخضع لإدارتها جميع خدمات وشبكات اتصالات أي مشغل أو مقدم خدمة، وأن تستدعي العاملين القائمين على التشغيل والصيانة، وذلك في الكوارث أو التعبئة العامة أو أي حالات أخرى تتعلق بالأمن القومي.

ذلك ما حدث مثلًا في عام 2013 حين أصدرت محكمة القضاء الإداري حكمها بحجب موقع يوتيوب لمدة شهر، وحجب جميع الروابط التي تعرض فيلم مسيء للرسول، معتمدة في ذلك على تفسيرها الواسع لنص المواد (64) و(67) من قانون تنظيم الاتصالات، حيث استطاعت المحكمة بواسطة هذه النصوص أن تجد مسوغاً قانونياً يمكن عن طريقه إلزام الجهات الإدارية بحجب المحتوى، وذلك من خلال التوسع في تفسير مفهوم الأمن القومي وضرورة حمايته.[22]

على ما سبق فإن البنية التشريعية المتداخلة للحجب في مصر تعمل كمنظومة تقييد متعددة المسارات تتوزع بين قوانين تُركّز على المحتوى وقوانين تُركّز على البنية التحتية وقوانين تتعامل مع الأوضاع الاستثنائية. وبالتالي فإن قرار الحجب يُمكن إنتاجه عبر أكثر من مدخل، أولها مدخل جنائي يربط الحجب بمنع أثر جريمة، وثانيها، مدخل تنظيمي يُقدِّم الحجب كأداة إدارة للمجال الإعلامي، وثالثها مدخل بنيوي يمنح الدولة قدرة التحكم في الشبكة ذاتها.

[21] مادة (19): يحظر على الصحيفة أو الوسيلة الإعلامية أو الموقع الإلكتروني نشر أو بث أخبار كاذبة، أو ما يدعو أو يحرض على مخالفة القانون أو إلى العنف أو الكراهية، أو ينطوي على تمييز بين المواطنين، أو يدعو إلى العنصرية أو يتضمن طعنا في أعراض الأفراد، أو سبا أو قذفا لهم، أو امتهانا للأديان السماوية أو للعقائد الدينية.
ويلتزم بأحكام الفقرة السابقة كل موقع إلكتروني شخصي أو مدونة إلكترونية شخصية أو حساب إلكتروني شخصي، يبلغ عدد متابعيه خمسة آلاف متابع أو أكثر.
ومع عدم الإخلال بالمسئولية القانونية المترتبة على مخالفة أحكام هذه المادة، يجب على المجلس الأعلى اتخاذ الإجراء المناسب حيال المخالفة، وله في سبيل ذلك وقف أو حجب الموقع أو المدونة أو الحساب المشار إليه بقرار منه.
ولذوي الشأن الطعن على القرار الصادر بذلك أمام محكمة القضاء الإداري.

[22] الحجب أداة رقابة مستقرة في التشريعات المصرية، مؤسسة مسار، ديسمبر 2021، الرابط: https://masaar.net/ar/%d8%a7%d9%84%d8%ad%d8%ac%d8%a8-%d8%a3%d8%af%d8%a7%d8%a9-%d8%b1%d9%82%d8%a7%d8%a8%d8%a9-%d9%85%d8%b3%d8%aa%d9%82%d8%b1%d8%a9-%d9%81%d9%8a-%d8%a7%d9%84%d8%aa%d8%b4%d8%b1%d9%8a%d8%b9%d8%a7%d8%aa-%d8%a7/



شكل (5): المداخل القانونية الثلاثة للحجب

وهذا التشظي يضعف شرط القابلية للتوقع، فالفاعل الرقمي لا يعرف مسبقًا أي معيار سيُطبَّق وأي جهة ستتحرك وبأي إجراءات، وهو ما يحوّل الحق في النفاذ إلى المعلومات من قاعدة إلى وضع قابل للتعليق، ويجعل منطق الاستثناء حاضرًا حتى في السياقات التي لا تستدعيه بطبيعتها.

> **«يتحول الحق في النفاذ إلى المعلومات من قاعدة إلى وضع قابل للتعليق»**

ومن زاوية الضمانات، فإن تحويل الحجب إلى فعل إجرائي لا يحسم مسألة المشروعية الدستورية بحد ذاته؛ لأن جوهر الحماية لا يتوقف على وجود خطوات شكلية (عرض/تصديق/تسبيب) بقدر ما يتوقف على ضيق المعيار وفعالية الرقابة واستقلالها وحدود الأثر.

وفي سياق وجود مفاهيم واسعة مثل الأمن القومي أو الخطر الوشيك دون تعريفات منضبطة، تصبح الرقابة القضائية -حتى عندما تُستدعى- محكومة بطبيعة معيار قابل للتوسع في التفسير. كما أن تحميل مقدمي الخدمة دور التنفيذ الفوري يخلق ميلًا إلى الامتثال المفرط وتوسيع نطاق الحجب لتجنب المسؤولية، بما يزيد مخاطر الحجب الزائد ويمس حق الجمهور في المعرفة ويفرض أثرًا من الرقابة الذاتية.

ثالثًا: أزمة تراخيص المواقع الإلكترونية الصحفية في مصر

تتمثل أزمة التراخيص في أن قطاعًا واسعًا من المواقع الصحفية المستقلة والمبادرات الرقمية يعمل داخل مصر في وضع قانوني هش، لأن "الوجود الرقمي" ذاته جرى ربطه بشرط إداري سابق هو الحصول على ترخيص. وعلى ذلك فإن الترخيص أقرب إلى شرط وجود لا إلى تنظيم مهني محدود؛ إذ يمكن التعامل مع موقع قائم بوصفه نشاطًا "غير مشروع" لمجرد غياب التصريح، بما يفتح الباب أمام إجراءات تمس استمراريته حتى قبل مناقشة أي مخالفة مهنية محددة.

«الترخيص أقرب إلى شرط وجود لا إلى تنظيم مهني محدود»

ويرتبط التنظيم القانونى لتراخيص المواقع الإلكترونية في مصر بثلاثة تشريعات:

- قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام رقم 180 لسنة 2018 والذي يتضمن القواعد العامة الحاكمة لترخيص المواقع الإلكترونية وخاصة المواقع الإلكترونية العاملة في مجالات الصحافة والإعلام والإعلان،
- ويحيل قانون تنظيم الإعلام الضوابط الإجرائية إلى اللائحة التنفيذية للقانون الصادرة بقرار رئيس مجلس الوزراء رقم 418 لسنة 2020
- كما يحيل التفاصيل التطبيقية المتعلقة بالرسوم ونماذج التراخيص إلى لائحة تنظيم التراخيص بالمجلس الأعلى لتنظيم الإعلام والصادرة بقرار المجلس الاعلى لتنظيم الإعلام رقم 26 لسنة 2020.

على مستوى قانون تنظيم الإعلام يقرر المُشرِّع ابتداءً شمول أحكامه للكيانات والمؤسسات والوسائل الصحفية والإعلامية والمواقع الإلكترونية، مع استثناءات محددة للحساب أو الموقع الشخصي، ويُلزم الكيانات القائمة بتوفيق الأوضاع خلال ستة أشهر من تاريخ العمل باللائحة التنفيذية وفق حكم المادة الثانية من مواد الإصدار.

ثم يضع القاعدة العامة المتعلقة بتراخيص المواقع الإلكترونية في المادة (6)[23] التي تقرر أنه لا يجوز تأسيس مواقع إلكترونية في جمهورية مصر العربية أو إدارتها، أو إدارة مكاتب أو فروع لمواقع تعمل من خارج الجمهورية، إلا بعد الحصول على ترخيص من المجلس الأعلى وفق الضوابط والشروط التي يضعها المجلس.

ويربط النص الترخيص بأثرٍ إداري لاحق عند المخالفة، إذ يجيز للمجلس مع عدم الإخلال بالعقوبات الجنائية اتخاذ الإجراءات اللازمة عند مخالفة أحكام الترخيص أو عدم الحصول عليه، بما في ذلك إلغاء الترخيص أو وقف نشاط الموقع أو حجبه، وبهذا يُفهم أن الترخيص في قانون تنظيم الصحافة والإعلام هو آلية تنظيم المحتوى الرقمي وربط استمرارية التشغيل بامتثالٍ إداري.

أما على مستوى اللائحة التنفيذية لقانون تنظيم الإعلام، فهي تفصل هذا الإطار العام إلى خطوات زمنية ونماذج ورسوم وحدود اختصاص. فتقرر اللائحة -ضمن أحكام إنشاء وتشغيل الوسائل الإعلامية والمواقع الإلكترونية- أن المجلس يضع النماذج اللازمة

[23] المادة (6): لا يجوز تأسيس مواقع إلكترونية في جمهورية مصر العربية، أو إدارتها، أو إدارة مكاتب أو فروع لمواقع إلكترونية تعمل من خارج الجمهورية، إلا بعد الحصول على ترخيص بذلك من المجلس الأعلى وفق الضوابط والشروط التي يضعها في هذا الشأن.
ومع عدم الإخلال بالعقوبات الجنائية المقررة، للمجلس الأعلى في حالة مخالفة أحكام الفقرة السابقة اتخاذ الإجراءات اللازمة بما في ذلك إلغاء الترخيص، أو وقف نشاط الموقع أو حجبه، في حالة عدم الحصول على ترخيص سار.
ولذوي الشأن الطعن على القرار الصادر بذلك أمام محكمة القضاء الإداري.

لطلبات إنشاء أو تشغيل الوسائل الإعلامية، وأن هذه النماذج تتضمن بيانات تفصيلية عن المالك والممثل القانوني، واللغة، وطبيعة النشاط، ومصادر التمويل، والهيكل الإداري والتحريري، ومسؤول البث ومدير البرامج، ومكان البث.

وإدراج عناصر مثل مصادر التمويل والهيكل التحريري يضع الاستقلال المؤسسي للمبادرات الرقمية ضمن نطاق تقييم إداري، ويُنتج قابلية لاستخدام "متطلبات الإفصاح" كوسيلة ضغط أو تعطيل، خصوصًا في بيئة يتسم فيها المجال الإعلامي بحساسية سياسية عالية.

ثم تنتقل اللائحة إلى الضوابط المالية والزمنية، إذ تنص المادة (11)[24] من اللائحة التنفيذية على أن طلب إنشاء أو تشغيل الوسيلة الإعلامية أو الموقع الإلكتروني يقدم إلى الأمانة العامة للمجلس على النموذج المعد لهذا الغرض، ويرفق به إيصال سداد رسم محدد؛ وتذكر صراحة أن الرسم قدره 50 ألف جنيه للموقع الإلكتروني. وتُحال الطلبات إلى لجنة التراخيص المختصة خلال أسبوع من ورودها، وتُلزم اللجنة بإعداد تقرير بالرأي خلال ثلاثين يومًا من تاريخ إحالة الطلب، ثم يعرض التقرير على المجلس للنظر في إصدار الترخيص أو رفضه.

وتحدد المادة (12)[25] أن قرار المجلس بالترخيص أو الرفض يصدر خلال تسعين يومًا من تاريخ ورود الطلب مستوفيًا البيانات والمستندات، ويُخطر مقدم الطلب بكتاب موصى عليه بعلم الوصول، إلا أن هذا الموعد أمر تنظيمي لا يترتب على مخالفته أي أثر، وذلك على خلاف النصوص المنظمة للصحافة الورقية التي تعتبر سكوت المجلس عن الرد على الطلبات المقدمة خلال المدة المحددة موافقة ضمنية على منح الترخيص.

وتظهر إشكاليات مع الشروط المالية والزمنية. فالرسوم المرتفعة لطلبات تشغيل المواقع تُنتج حاجز دخول واقعيًا أمام المبادرات الصغيرة والمشروعات المستقلة، وتحوّل الترخيص إلى كلفة تأسيس لا تتناسب مع طبيعة النشر الرقمي منخفض الكلفة في الأصل.

[24] المادة (11) من قرار رئيس مجلس الوزراء رقم 418 لسنة 2020 بإصدار اللائحة التنفيذية لقانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام

"يقدم طلب إنشاء أو تشغيل الوسيلة الإعلامية أو الموقع الإلكترونى إلى الأمانة العامة للمجلس الأعلى على النموذج المعد لهذا الغرض، ويرفق به إيصال سداد رسم مقداره مائتين وخمسين ألف جنيه بالنسبة للوسيلة الإعلامية، وخمسين ألف جنيه بالنسبة للموقع الإلكترونى.

وتقيد الأمانة العامة الطلبات المقدمة إليها فى سجل خاص يعد لذلك الغرض يسجل فيه ما تم فى كل طلب.

وتحيل الأمانة العامة الطلبات إلى لجنة التراخيص المختصة بالمجلس الأعلى خلال أسبوع من تاريخ ورود الطلب إليها، وتعد لجنة التراخيص المختصة تقريرًا برأيها فى الطلب بعد فحصه ويعرض تقريرها على المجلس الأعلى خلال ثلاثين يومًا من تاريخ إحالة الطلب إليها، وذلك للنظر فى إصدار الترخيص من عدمه وتكون مدة الترخيص خمس سنوات يجوز تجديدها بناءً على طلب يقدم من المرخص له إلى المجلس الأعلى قبل ستة أشهر من انتهائه، ويكون تجديد الترخيص مقابل سداد رسم بالقيمة ذاتها المنصوص عليها بالفقرة الأولى من هذه المادة وبعد مراجعة شروط تجديده."

[25] المادة (12) من قرار رئيس مجلس الوزراء رقم 418 لسنة 2020 بإصدار اللائحة التنفيذية لقانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام

"إذا كانت بيانات طلب الترخيص غير مستوفاة، فيجب على المجلس الأعلى إخطار مقدم الطلب لاستيفائها وذلك خلال ثلاثين يومًا من تاريخ عرض تقرير لجنة التراخيص عليه، ويكون الإخطار بكتاب مسجل موصى عليه بعلم الوصول.

ويصدر المجلس الأعلى قراره فى الطلب بالترخيص أو برفضه بموافقة أغلبية أعضائه الحاضرين وذلك خلال ثلاثين يومًا من تاريخ عرض تقرير لجنة التراخيص عليه، ويكون الإخطار بكتاب مسجل موصى عليه بعلم الوصول.

ويصدر المجلس الأعلى قراره فى الطلب بالترخيص أو برفضه بموافقة أغلبية أعضائه الحاضرين وذلك خلال تسعين يومًا من تاريخ وروده إليه مستوفيًا كافة البيانات والمستندات، ويخطر مقدم الطلب بقرار المجلس الأعلى بكتاب مسجل موصى عليه بعلم الوصول.

ولذوى الشأن الطعن فى قرار المجلس الأعلى أمام محكمة القضاء الإدارى"

كما أن مدد فحص الطلبات وإصدار القرار -حتى مع تنظيمها في اللائحة- لا تقترن بآلية فعالة تمنع تعطيل الطلبات بالسكوت؛ إذ لا يترتب على عدم الرد خلال المدة أثر "موافقة ضمنية" كما هو الحال في بعض النظم الأكثر حماية للتعددية.

كما توضح اللائحة التنفيذية أن مدة الترخيص هي خمس سنوات قابلة للتجديد بطلب يُقدم قبل الانتهاء بستة أشهر، ويكون التجديد مقابل سداد الرسم ذاته بعد مراجعة الشروط. وتلزم اللائحة التنفيذية وفقًا للمادة (16)[26] الوسائل الإعلامية والمواقع الإلكترونية المرخص لها بالاحتفاظ بكافة المواد التي تم بثها لمدة لا تقل عن سنة، مع إيداع نسخة للمجلس، وتلزم كذلك بوجود نسخة من الخوادم الإلكترونية التي تستضيف النسخة الإلكترونية داخل جمهورية مصر العربية في مكان "آمن ومعلوم للمجلس"، وعدم تغييرها إلا بعد موافقة المجلس.

هذه الاشتراطات قد تبدو منطقية تنظيميًا، لكنها تتجاوز فكرة "الترخيص" إلى التزامات تشغيلية مستمرة مثل أرشفة المحتوى، وإيداع نسخة لدى المجلس، وتوطين الخوادم داخل مصر في نطاق معلوم له. وهذا قد يسهّل الرجوع إلى الأرشيف وتنفيذ أي تدابير تنظيمية لاحقة دون أن يعني بالضرورة رقابة مباشرة. لكن في المقابل، يرفع حساسية أمن الأرشيف والبيانات التشغيلية، بما يستلزم ضمانات أوضح لحدود الطلبات وإجراءاتها وحق الطعن لتقليل مخاطر التعسف أو التسريب.



شكل (6): مراحل ترخيص المواقع الإلكترونية وأعباؤه

[26] المادة (16) من قرار رئيس مجلس الوزراء رقم 418 لسنة 2020 بإصدار اللائحة التنفيذية لقانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام:

يجب على الوسائل الإعلامية والمواقع الإلكترونية المرخص لها الاحتفاظ بكافة المواد التى تم بثها لمدة لا تقل عن سنة من تاريخ البث، وتلتزم بإيداع نسخة منها بالمجلس الأعلى شهريًا، كما يجب أن توجد نسخة من الخوادم الإلكترونية التى تستضيف النسخة الإلكترونية فى مكان تحدده الوسيلة الإعلامية أو الموقع الإلكتروني داخل جمهورية مصر العربية شريطة أن يكون آمنًا ومعلومًا للمجلس الأعلى، ولا يجوز تغييره إلا بعد موافقة المجلس الأعلى.

أما لائحة تنظيم التراخيص -وفقًا للمادة 5[27]- تقرر أن نماذج التراخيص الصادرة من المجلس الأعلى تحدد الحقوق والالتزامات والاشتراطات التي لا يجوز مخالفتها وتعد جميعها شروطًا جوهرية من شروط الترخيص. وتعطي مساحة واسعة وتقديرية في وضع ضوابط منح التراخيص ووضع نماذج قبول طلبات الترخيص.

وطبقًا لما سبق فإن منظومة الترخيص تعمل كآلية تحويل الوجود الصحفي الرقمي إلى وجود مشروط بإذن إداري قابل للسحب. وبمجرد ربط المشروعية بالترخيص، يصبح عدم الحصول عليه -أو أي خلاف حول استمراره- مدخلًا جاهزًا لتفعيل أدوات الإيقاف والحجب خارج منطق المساءلة اللاحقة على محتوى محدد. بذلك يتحول الترخيص من إجراء تأسيسي إلى وسيلة انضباط مستمرة تمكّن السلطة التنظيمية من التحكم في استمرارية المنصات المستقلة، وتوسّع عمليًا من قابلية استخدام الحجب كأداة إدارة للمجال العام الرقمي، لا كإجراء استثنائي محدود.

[27] (مادة 5) من قرار رقم 26 لسنة 2020 بإصدار لائحة تنظيم التراخيص بالمجلس الأعلى لتنظيم الإعلام " تُحدد نماذج التراخيص الصادرة من المجلس الأعلى كافة الحقوق والالتزامات والاشتراطات التى لا يجوز مخالفتها، وتُعد جميعها شروطًا جوهرية من شروط الترخيص "

رابعًا: التوسع في تجريم وحيازة واستخدام معدات الاتصالات

أحدثت تعديلات قانون تنظيم الاتصالات المصري في عام 2022 تحولًا نوعيًا في القانون، حين وافق مجلس الوزراء على مشروع تعديل[28] يهدف إلى تغليظ العقوبات المرتبطة بحيازة واستخدام أجهزة تقوية المحمول غير الشرعية ضمن خطة "ضبط منظومة الاتصالات".

هذه الصياغة تضع ظاهرة محددة في المقدمة، لكنها تُنتج حلًا تشريعيًا عامًا يتجاوز الظاهرة ويؤسس لقاعدة قابلة للتمدد. بعد ذلك، سلك المشروع طريقه إلى مجلس النواب، وأُقرّت الصيغة النهائية، وفي نهاية ديسمبر صدر تعديل قانون تنظيم الاتصالات بالقانون رقم 172 لسنة 2022.[29]

تمحور التعديل حول استبدال نصين هما الفقرة الأولى من المادة (44) والمادة (77) من القانون.[30] وبموجب الصياغة الجديدة، لم يعد الحظر مقصورًا على مراحل إدخال المعدات إلى السوق (كالاستيراد أو التصنيع أو التجميع)، بل امتدّ ليشمل أفعالًا تقع في قلب الممارسة اليومية مثل الحيازة، والاستخدام، والتشغيل، والتركيب، والتسويق.

[28] جريدة الشروق، الحكومة توافق على تعديل أحكام بـ تنظيم الاتصالات وتغليظ عقوبات حيازة أجهزة تقوية المحمول، يوليو 2022، الرابط: https://www.shorouknews.com/news/view.aspx?cdate=28072022&id=e654a0cf-d8e4-4639-b3fa-b69e8b2ebbfc

[29] صدر تعديل قانون تنظيم الاتصالات برقم 172 لسنة 2022 ونُشر في الجريدة الرسمية (العدد 51 مكرر "هـ" بتاريخ 26 ديسمبر 2022)الرابط: 49930/123456789/https://mediadr.sis.gov.eg/handle

[30] نص التعديلات كما نشر بالجريدة الرسمية العدد 51 مكرر "هـ" بتاريخ 26 ديسمبر 2022
يستبدل بنصي المادتين /44 فقرة أولي، 77 من قانون تنظيم الاتصالات الصادر بالقانون رقم 10 لسنة 2003، النصان الآتيان:
مادة 44/ فقرة أولي:
يحظر استيراد أي معدة من معدات الاتصالات، أو تصنيعها، أو تجميعها، أو حيازتها، أو استخدامها، أو تشغيلها، أو تركيبها، أو تسويقها إلا بعد الحصول علي تصريح بذلك من الجهاز، طبقًا للمعايير والمواصفات وأنواع المعدات المعتمدة منه.
مادة 77:
مع مراعاة حكم الفقرة الأخيرة من المادة 48 من هذا القانون، يعاقب بالحبس مدة لا تقل عن سنة ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مليوني جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين كل من قام باستيراد، أو تصنيع، أو تجميع، أو تسويق أي معدة من معدات الاتصالات دون الحصول علي تصريح من الجهاز بالمخالفة للمادة /44 فقرة أولي من هذا القانون.
ويعاقب بالحبس وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من قام بحيازة، أو استخدام، أو تركيب، أو تشغيل أي معدة من معدات الاتصالات دون الحصول علي تصريح من الجهاز بالمخالفة للمادة /44 فقرة أولي من هذا القانون، ولا تسري هذه العقوبة في حالة الأجهزة اللاسلكية التي يصدر الجهاز ترخيصًا عامًا بحيازتها أو استخدامها أو تركيبها أو تشغيلها وبما لا يخل بأحكام المادة 44 من هذا القانون.
وتكون العقوبة السجن المشدد إذا كان الاستيراد، أو التصنيع، أو التجميع، أو الحيازة، أو التركيب، أو التشغيل أو الاستخدام أو التسويق للمعدات المخالفة للقانون بغرض المساس بالأمن القومي.
وتضاعف العقوبة المشار إليها بالفقرات الأولي والثانية والثالثة من هذه المادة في حديها الأدنى والأقصى في حالة العود.
وتقضي المحكمة في جميع الأحوال بمصادرة المعدات محل الجريمة ومكوناتها



شكل (7): نطاق الحظر قبل تعديل قانون الاتصالات 2022 وبعده

وبالتالي، لا يظل التنظيم محصورًا في حلقات إدخال المعدات إلى السوق، بل يمتد -بحكم النص- إلى مستوى الممارسة اليومية نفسها؛ لأن الحظر يشمل الحيازة والاستخدام والتشغيل والتركيب والتسويق.

ونتيجة هذا الاتساع أن متطلبات التصريح قد تمتد إلى أنشطة فنية روتينية ومشروعة في ذاتها -كالصيانة وإصلاح الأعطال والاختبار الميداني- متى اعتُبرت الأدوات المستخدمة داخلة ضمن "معدات الاتصالات". كما أن نطاق ما يُعدّ "معدات اتصالات" يرتبط عمليًا بالأنواع والمعايير التي يعتمدها الجهاز القومي لتنظيم الاتصالات، ما يجعل الامتثال متوقفًا على تصنيف تنظيمي قد يتسع أو يضيق.

وبالتالي فإن القاعدة الحالية لا تستهدف فقط المعدات عالية الخطورة أو الاستخدامات الضارة على نحو مباشر، بل تفتح مجالًا لأن تُعامل ممارسات تقنية شائعة باعتبارها محل اشتباه مسبق ما لم تُستوفَ متطلبات التصريح.

ومن الإشكاليات الأخرى أن النص يتعامل مع "معدات الاتصالات" ككتلة واحدة، بينما التقنيات ليست متساوية في مخاطرها ولا في وظائفها. فبعض المعدات قد تُستخدم للتداخل على الترددات أو تعطيل الشبكات أو تقويض سلامة الاتصالات، بينما غالبية المعدات أدوات تشغيل اعتيادية، أو أدوات فحص وصيانة، أو مكونات شبكات سلكية ولاسلكية، أو أجهزة قياس ومُلحقات لازمة لعمل الفنيين والباحثين. وعندما يُطبَّق المنطق الجنائي ذاته على هذا الطيف كله، يصبح القانون مولّدًا للتعسف وتتحول السيطرة على التقنية من استهداف المخاطر المحددة إلى ضبط عام يسبق الفعل ويُجرّم الحيازة والاستخدام والتشغيل والتركيب والتسويق.

ويزداد الأثر تضييقًا بسبب طريقة الإحالة إلى الجهاز القومي لتنظيم الاتصالات. فالنص يربط مشروعية الفعل بمعايير ومواصفات وأنواع "يعتمدها الجهاز". فيصبح الحد الفاصل بين المشروع وغير المشروع مرتبط عمليًا بقوائم ومعايير تنظيمية متغيرة، لا بتعريف تشريعي محدد ومستقر يمكن التعامل معه بسهولة. وبقدر ما تغيب الشفافية أو الإتاحة الميسرة لهذه القوائم والمعايير،

يصبح الامتثال عملية شاقة تقوم على التحقق المستمر من قرارات الجهاز، لا على قاعدة قانونية واضحة يمكن للمواطن أو الفني أو التاجر أو الباحث أن يفهمها بذاتها.

هذه النقطة مهمة لأننا أمام قاعدة ذات أثر جنائي، يتحول فيها التصنيف الإداري للمعدات إلى شرط لتجنب العقوبة، تتبدل العلاقة بين الفرد والقانون من "إباحة أصلية مع منع محدد" إلى "منع شامل مع استثناء مشروط"، بما يضعف القدرة على الامتثال ويجعل التقنية نفسها موضوعًا للتقييد قبل أن تكون وسيلة لممارسة حقوق أو نشاط اقتصادي أو بحثي مشروع.

كما أن اتساع النص يخلق انقلابًا في عبء الامتثال، وبدلًا من أن تُثبت السلطة أن معدات بعينها استُخدمت على نحو ضار أو أحدثت تداخلًا أو هددت الشبكات، يصبح على الأفراد والفاعلين التقنيين أن يثبتوا مسبقًا أن ما لديهم "مصرّح ومعتمد". وهذا التحول يُنتج أثرًا ردعيًا واسعًا حتى في غياب إنفاذ جنائي كثيف، لأن مجرد عدم اليقين بشأن نطاق "معدات الاتصالات" وما يدخل ضمن "المعتمد" كافٍ لخلق رقابة ذاتية لدى المستخدمين والفنيين، وتفادي اقتناء أو اختبار أو تداول معدات قد تكون ضرورية للعمل أو البحث أو الصيانة.

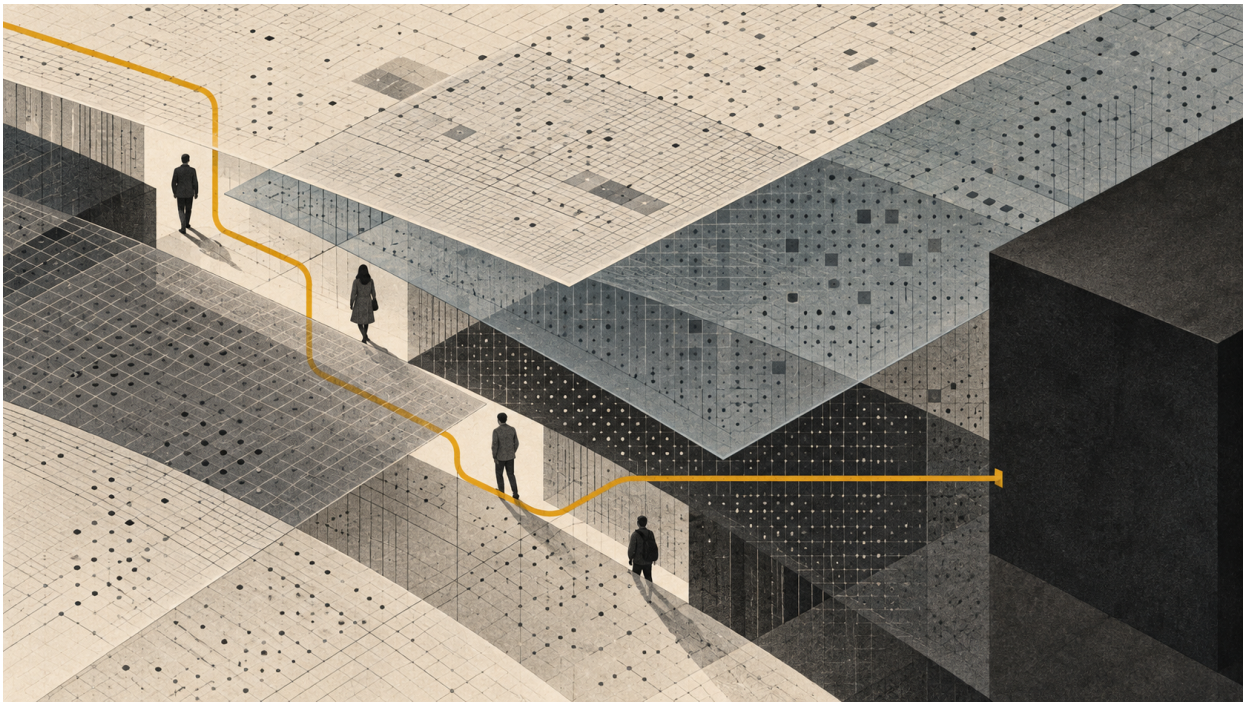
ويمتد الأثر أيضًا إلى المجال الاقتصادي والتقني، فأسواق الصيانة وقطع الغيار والبيع المستعمل والورش الصغيرة ومزودو الخدمات المحليون يعتمدون على تداول معدات وأجزاء ومُلحقات قد تُصنَّف -وفق تفسير واسع- ضمن معدات الاتصالات. وعندما تصبح هذه السوق خاضعة لخطر جنائي مرتبط بالتراخيص، تتضخم كلفة الامتثال مثل رسوم وتصاريح وإجراءات وتوقف محتمل عن العمل، وهو ما لا يتحمله الفاعلون الصغار بالتأكيد. وذلك ما يمكن أن يخلق تأثير احتكاري غير مباشر، حيث من يملك القدرة الإدارية والمالية على إدارة التصاريح والمعايير سيستمر، ومن لا يملكها سيتراجع أو يعمل تحت تهديد دائم.

وتظهر تبعات مشابهة على المجتمع البحثي والتعليمي، فالبحث في الشبكات وأمن المعلومات والاتصالات اللاسلكية يتطلب في كثير من الأحيان أدوات قياس وتجريب وتجميع وتعديل وتشغيل معدات متعددة. وحين يُوضع هذا النشاط داخل نطاق الاشتباه الجنائي المسبق، يصبح الابتكار التقني مشروطًا بموافقات قد تكون غير واضحة أو بطيئة، ويزداد الميل إلى تجنب مشاريع بحثية بعينها أو نقلها خارج المجال المحلي أو حصرها داخل مؤسسات كبيرة فقط.

ومن ناحية الإنفاذ، يرفع هذا البناء التشريعي مخاطر الاستهداف الانتقائي؛ لأن النص واسع، ولأن جزءًا كبيرًا من المعدات مزدوج الاستخدام، فإن تحديد المخالفة في الواقع العملي يمكن أن يصبح مرتبطًا بسياق الضبط والتفتيش والتقييم الإداري أكثر من ارتباطه بضرر ملموس. هذا النوع من الاتساع يخلق قابلية عالية للحجز والمصادرة والتجريم بناء على تقدير، ويزيد من هشاشة ضمانات الحماية للأعمال التقنية المشروعة التي لا تحمل خطرًا استثنائيًا.

المنطق الذي تسوقه الدولة عادةً في مثل هذه التعديلات يرتكز على مفردات الأمن القومي وحماية الشبكات من التداخل ومنع الاستخدامات غير المشروعة لمقوّيات الإشارة وغيرها. وهذا المنطق، من حيث المبدأ، لا يُرفض في ذاته. غير أن تقييمه من منظور الحقوق الرقمية لا يتوقف على الغاية المعلنة وحدها، بل على طبيعة القيد وأدواته وضماناته، مثل مدى وضوح القاعدة وتحديد نطاقها، وقدرتها على التمييز بين المعدات عالية الخطورة والمعدات الاعتيادية، وتوافر استثناءات عملية للصيانة والبحث والتجريب، وشفافية المعايير وسهولة إتاحتها وإمكانية الطعن عليها بصورة فعّالة، وترتيب الجزاءات بحيث تظل العقوبة الجنائية ملاذًا أخيرًا.

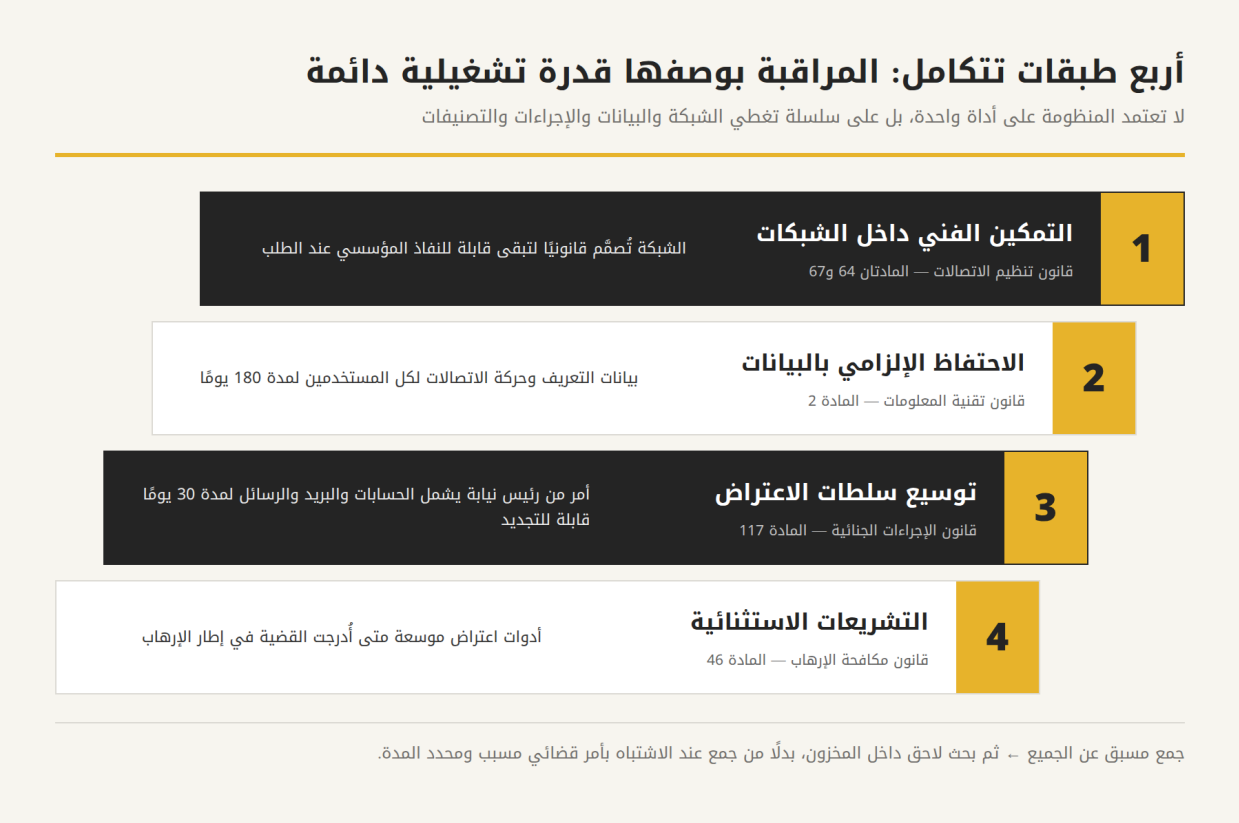
خامسًا: المراقبة الجماعية



تراكم طبقات جمع البيانات والاعتراض

البناء التشريعي المصري يعامل الرقابة الجماعية بوصفها **قدرة تشغيلية دائمة** تُدار عبر قواعد متراكمة مستمرة، وليس بوصفها تدخلًا عند الضرورة؛ أي أن الشبكات تُصمَّم قانونيًا لتبقى قابلة للنفاذ المؤسسي، وأن البيانات تُحفظ مسبقًا، وأن مسارات الاعتراض تُبسط إجرائيًا. هذا النوع من الترتيب يرفع مخاطر **التدخل الواسع** لأن القدرة، حين تُبنى كقاعدة تشغيل، تميل إلى الاتساع والتكرار حتى خارج نطاق الحالات الأشد خطورة.

ولفهم كيف تعمل هذه المنظومة، من المفيد النظر إلى المراقبة بوصفها طبقات تتكامل أكثر مما تتجاور، بحيث لا تعتمد الدولة على أداة واحدة (اعتراض محتوى مثلًا)، بل على سلسلة أدوات تغطي البنية التحتية (الشبكة)، والبيانات (الاحتفاظ)، والإجراءات (الأذونات)، والتصنيفات (قضايا الإرهاب)، ثم تُستكمل بحلقات أقل ظهورًا تتعلق بالمشاركة والتخزين والأمن المعلوماتي.



شكل (8): طبقات المراقبة الأربع وسندها التشريعي

الطبقة الأولى: التمكين الفني داخل الشبكات

الطبقة الأولى داخل الشبكات والبنية التحتية نفسها، وهي التي يضعها قانون تنظيم الاتصالات رقم 10 لسنة 2003 في (المادة 67) حيث تدخل أجهزة الأمن القومي في صميم التصميم القانوني للعلاقة بين الدولة ومشغلي الاتصالات.

في هذه الصياغة تصبح الشبكة مجالًا يجب أن يبقى قابلًا للنفاذ المؤسسي عند الطلب، وهو ما يحول النقاش من مجرد سؤال وجود مراقبة من عدمه إلى الكيفية التي تم بها بناء القدرة على المراقبة داخل البنية التحتية ذاتها. ويترتب على ذلك أن قيمة الضمانات لا تتوقف على إعلان المبادئ العامة، بل على حدود الطلبات وتوثيقها والرقابة المستقلة على استخدامها، وذلك غير موجود في مصر.

الطبقة الثانية: الاحتفاظ الإلزامي بالبيانات كقاعدة

يفرض قانون مكافحة جرائم تقنية المعلومات (المادة 2)[31] التزامًا على مقدمي الخدمة بالاحتفاظ ببيانات الاستخدام لمدة 180 يومًا، بما يشمل بيانات التعريف وبيانات حركة الاتصالات وما يتصل بها من معلومات تسمح بتتبع الأنماط والعلاقات. ما يستحق

[31] المادة (2)
إلتزامات وواجبات مقدم الخدمة
أولاً: مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم 10 لسنه 2003 الْمُشار إليه، يلتزم مقدمو الخدمة بما يلى:
(1) حفظ وتخزين سجل النظام المعلوماتى أو أى وسيلة لتقنية المعلومات لمدة 180 يوما متصلة وتتمثل البيانات الواجب حفظها وتخزينها فيما يلى:
أ- البيانات التى تمكن من التعرف على مستخدم الخدمة.
ب – البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتى المتعامل متى كانت تحت سيطرته.
ج – البيانات المتعلقة بحركة الاتصال
د- البيانات المتعلقة بالاجهزة الطرفية للأتصال.
هـ – أى بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز.

إبرازًا هنا هو أن هذه البيانات -حتى عندما لا تشمل المحتوى- لا تُعد منخفضة الحساسية؛ لأن الميتاداتا (المصدر/الوجهة/الوقت/المدة/نوع الخدمة... إلخ) قادرة على رسم خريطة دقيقة للحياة الرقمية مثل دوائر التواصل، وأنماط الحركة ونقاط الاتصال المتكررة، وارتباطات الاهتمام.

«تتحول المراقبة من جمع عند الاشتباه إلى جمع مسبق عن الجميع ثم بحث لاحق داخل المخزون»

بذلك تتحول المراقبة من جمع عند الاشتباه وبأمر قضائي مسبب ومحدد المدة إلى جمع مسبق عن الجميع ثم بحث لاحق داخل المخزون. وهذا النمط يرفع مخاطر التعسف لأنه يجعل التدخل واسع النطاق افتراضيًا ويترك مسألة من يُفحص ولماذا لقرارات لاحقة لا تكون شفافة أو قابلة للطعن. ويمتد الأثر التشريعي لهذا النص إلى أن الاحتفاظ بالبيانات ليس قرارًا فقط سياسات تجارية أو سياسة خصوصية، بل التزام يعرّض الشركة للمساءلة إذا لم تنفذه لأن القانون نفسه يجعل البيانات موجودة وجاهزة للاستخدام.

الطبقة الثالثة: توسيع سلطات الاعتراض داخل الإجراءات الجنائية

توسيع سلطات الاعتراض داخل منظومة الإجراءات الجنائية، لا يقتصر على توسيع وسائل التحقيق، بل على نقل مركز الثقل نحو مسارات تسمح بتطبيع الاعتراض داخل التحقيقات، خصوصًا عندما تصبح سلطة إصدار الأوامر بيد جهة أقرب إلى منظومة التحقيق اليومية، وبمعايير تقديرية أوسع.

فقد شملت تعديلات قانون الإجراءات الجنائية الجديد نصوصًا تمنح النيابة سلطات تقديرية واسعة تتعلق بالحبس الاحتياطي واعتراض الاتصالات وحظر السفر حيث نقل مركز الثقل من رقابة قضائية صارمة إلى سلطة النيابة العامة -درجة قضائية أقل- وهو يعني توسيع نطاق مراقبة الاتصالات وتحويله من إجراء محدد بزمن وسبب إلى ممارسة يمكن تطبيعها داخل التحقيقات.[32]

(2) المحافظة على سرية البيانات التى تم حفظها وتخزينها، وعدم افشائها أو الافصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة – ويشمل ذلك البيانات الشخصية لأى من مستخدمى خدمته أو أى بيانات أو معلومات متعلقه بالمواقع والحسابات الخاصة التى يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التى يتواصلون معها.
(3) تأمين البيانات والمعلومات بما يحافظ على سريتها، وعدم اعتراضها أو اختراقها أو تلفها.
ثانيا: مع عدم الإخلال بأحكام قانون حماية المستهلك الصادر بالقانون رقم 67 لسنه 2006، يجب على مقدم الخدمة أن يوفر لمستخدمى خدماته ولأى جهة حكومية مختصة، فى الشكل، وبالطريقة التى يمكن الوصول إليها بصورة ميسرة ومباشرة ومستمرة، البيانات والمعلومات الاتية:
(1) اسم مقدم الخدمة وعنوانه.
(2) معلومات الاتصال المتعلقة بمقدم الخدمة، بما فى ذلك عنوان الاتصال الاليكترونى.
(3) بيانات الترخيص لتحديد هوية مقدم الخدمة، وتحديد الجهة المختصة التى يخضع لاشرافها.
(4) أيه معلومات أخرى يقدر الجهاز أهميتها لحماية مستخدمى الخدمة، ويحددها قرار من الوزير المختص.
ثالثا: مع مراعاة حرمة الحياة الخاصة التى يكفلها الدستور، يلتزم مقدمو الخدمة والتابعون لهم، أن يوفروا حال طلب جهات الأمن القومى، ووفقا لاحتياجاتها كافة الإمكانيات الفنية التى تتيح لتلك الجهات ممارسة اختصاصاتها وفقا للقانون.
رابعاً: يلتزم مقدمو خدمات تقنية المعلومات ووكلائهم وموزعيهم التابعون لهم المنوط بهم تسويق تلك الخدمات بالحصول على بيانات المستخدمين ويحظر على غير هؤلاء القيام بذلك.

[32] المواد رقم 114 و 117 و 531 من قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

الطبقة الرابعة: التشريعات الاستثنائية تحت مظلة مكافحة الإرهاب

الطبقة الرابعة تتمثل في التشريعات ذات الطابع الاستثنائي التي ترفع سقف التدخل تحت مظلة مكافحة الإرهاب. يمنح قانون مكافحة الإرهاب رقم 94 لسنة 2015 في المادة 46[33] أدوات موسعة لاعتراض الاتصالات والمراقبة، ويضيف شرعية أوسع لهذه التدابير عندما تُدرج القضايا في إطار جرائم الإرهاب.

ومع اتساع تعريفات الإرهاب والترويج له، تصبح مساحة إدراج أنشطة رقمية أو تواصل سياسي أو صحفي داخل هذا الإطار أكبر، فتُستدعى أدوات الاعتراض بصيغة تبدو قانونية، بينما تتسع في الواقع دائرة الاشتباه والتدخل.

وتتكامل هذه الطبقات مع فجوة تتعلق بالضمانات والمساءلة وأمن البيانات. فالاحتفاظ الإلزامي يخلق مخزونًا ضخمًا من البيانات الحساسة، ما يرفع مخاطر سوء الاستخدام أو التوسع في النفاذ، كما يرفع كذلك مخاطر التسريب أو الاختراق، وهي مخاطر لا تنفصل عن حماية الخصوصية ذاتها. كما أن تراكم الصلاحيات بين جهات متعددة، وتعدد المسارات القانونية الممكنة للنفاذ، يقلل من وضوح الحدود العملية للتدخل ويضعف قابلية التتبع والمراجعة المجتمعية الفعّالة.

في هذا السياق يصبح الحديث عن الخصوصية دون تحليل قواعد الاحتفاظ بالبيانات ومسارات النفاذ والرقابة على الاستخدام حديثًا غير مكتمل، لأن سقف الحقوق الرقمية يتحدد عمليًا بمدى انضباط هذه البنية عمليًا وليس بوجود الحق في النصوص وحدها.

[33] المادة 46 من قانون مكافحة الإرهاب رقم 94 لسنة 2015

"للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في جريمة إرهابية أن تأذن بأمر مسبب لمدة لا تزيد على ثلاثين يوماً، بمراقبة وتسجيل المحادثات والرسائل التي ترد على وسائل الاتصال السلكية واللاسلكية وغيرها من وسائل الاتصال الحديثة، وتسجيل وتصوير ما يجري في الأماكن الخاصة أو عبر شبكات الاتصال أو المعلومات أو المواقع الإلكترونية وما يدون فيها، وضبط المكاتبات والرسائل العادية أو الإلكترونية والمطبوعات والطرود والبرقيات بجميع أنواعها. ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مدداً أخرى"

سادسًا: ضعف قواعد حماية البيانات الشخصية

صدر قانون حماية البيانات الشخصية رقم 151 لسنة 2020 بوصفه أول إطار شامل نسبيًا لتنظيم التعامل مع البيانات الشخصية في مصر. من حيث البناء النظري، يُقدّم القانون نفسه كمنظومة تقرر مبادئ للمعالجة المشروعة، وتمنح صاحب البيانات حقوقًا، وتُلزم المتحكمين والمعالجين بواجبات تأمينية وإجرائية.

غير أن تقييم قوة الحماية لا يتوقف على وجود هذه المبادئ وحدها، بل على قابلية إنفاذها وحدود الاستثناءات التي تُقيّدها، وطبيعة الجهة المنوط بها تطبيقها، ومدى استقلالها وشفافية عملها. فالقانون يخلق ظهيرًا قويًا وجديدًا للخصوصية، لكنه في الوقت نفسه يبني استثناءات إنفاذ تجعل الخصوصية حقًا قابلًا للتعليق بسهولة عندما تُستدعى اعتبارات الأمن، وعندما تغيب الرقابة المستقلة والشفافية كشرطين لتفعيل الحماية.

ويظهر ذلك في نطاق الاستثناءات الواردة بالمادة الثالثة[34] من مواد إصدار القانون. فالمادة تستبعد من التطبيق، ضمن ما تستبعد، البيانات المعالجة للاستخدام الشخصي، والبيانات المعالجة لأغراض إحصائية رسمية أو تنفيذًا لنص قانوني، والبيانات المعالجة حصرًا للأغراض الإعلامية بشروط، والبيانات المتعلقة بمحاضر الضبط والتحقيقات والدعاوى. ثم تضع استثناءً واسعًا للبيانات لدى جهات الأمن القومي وما تقدره لاعتبارات أخرى.

ويضع القانون آلية تمنح جهات الأمن القومي تأثيرًا مباشرًا على تداول البيانات لدى جهات أخرى؛ إذ يوجب على مركز حماية البيانات، بناء على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات خلال مدة محددة، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار.

«تُذكر الخصوصية كحق، ثم تُفتح بوابات استثناء تجعل سقف الحماية مرتبطًا ببنية السلطة ومساراتها»

كما يظهر استثناء آخر وهو البيانات التي يحوزها البنك المركزي أو الجهات المرخص لها العمل في مصر من البنك المركزي (القطاع المصرفي والقطاع المالي غير المصرفي) ما يعني خروج قطاع كامل من المنظومة العامة لحماية البيانات ليُنتج تفاوتًا في مستويات الحماية والإنفاذ تبعًا للجهة الحائزة للبيانات، ويقيد عمليًا قدرة الأفراد على استخدام مسارات الحماية العامة أمام جهة مستثناة.

[34] مادة 3: لا تسري أحكام القانون المرافق علي ما يأتي:
1 – البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي.
2 – البيانات الشخصية التي تتم معالجتها بغرض الحصول علي البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني.
3 – البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخري، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.
4 – البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوي القضائية.
5 – البيانات الشخصية لدي جهات الأمن القومي، وما تقدره لاعتبارات أخري. ويجب علي المركز، بناءً علي طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به.
6 – البيانات الشخصية لدي البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة، علي أن يراعي في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية.



شكل (9): الاستثناءات الواردة على نطاق قانون حماية البيانات الشخصية

أما ما يتعلّق باللائحة التنفيذية للقانون، فبدلًا من أن تركز على ضمانات شفافة ومحددة تُقيّد تداول البيانات وتمنح صاحبها مسارات واضحة للشكاوى، تُدخل اللائحة شبكة واسعة من المتطلبات التنظيمية السابقة، مثل اشتراط الحصول على ترخيص أو تصريح بوصفه متحكمًا أو معالجًا، وربط جمع البيانات بموافقات وآليات يعتمدها المركز. [35]

وهذا التصميم القانوني قد يُفهم تنظيميًا بوصفه محاولة لضبط السوق، لكنه في الوقت نفسه يجعل الحماية مرتبطة بامتثال إداري كثيف، ويمنح الجهة التنظيمية دورًا واسعًا في اعتماد الآليات والمعايير، ما يثير أسئلة تتعلق بمدى الاستقلال وعلنية القرارات واتساق المعايير وقابلية الطعن الفعال على قرارات الاعتماد والترخيص.

وتظهر أيضًا تحفظات على كيفية إدارة خروقات البيانات كما وردت في اللائحة التنفيذية. فاللائحة تفرض الإبلاغ عن خرق/انتهاك البيانات، وتضيف مسارًا خاصًا عندما تكون الواقعة "ذات صلة باعتبارات حماية الأمن القومي"، مع إلزام بالإبلاغ الفوري، ثم تلزم المركز بإتاحة وسيلة اتصال خاصة لتلقي البلاغات المتعلقة باعتبارات الأمن القومي، وبالتنسيق مع جهات الأمن القومي لتحديد آليات إخطارها حال تلقي البلاغات.

هذه القواعد لا تنفي وجود التزام بالإخطار لصاحب البيانات، لكنها تُظهر أن إدارة الخروقات لا تُفهم فقط كمسار حماية للأفراد، بل تتضمن قناة مؤسسية موازية ذات طابع أمني في حالات بعينها، وهو ما قد يغيّر توازنات الشفافية وطبيعة المعلومات المتداولة حول الواقعة وحدودها.[36]

[35] اللائحة التنفيذية لقانون حماية البيانات الشخصية: اختبار تحويل القواعد العامة إلى التزامات قابلة للمساءلة، مؤسسة مسار والمبادرة المصرية للحقوق الشخصية، فبراير 20226، الرابط: https://masaar.net/ar/testing-the-executive-regulations-data-protection-law/

[36] المصدر السابق

يظهر أثر آخر لا يقل خطورة في الاستثناءات المتعلقة بالعمل الصحفي والإعلامي. القانون يستثني معالجة البيانات للأغراض الصحفية أو الإعلامية بشرط الدقة وعدم الاستخدام لأغراض أخرى، مع التأكيد على عدم الإخلال بقوانين تنظيم الصحافة والإعلام.

ولا يبدو هذا الاستثناء يعمل كحماية مستقلة لبيئة الصحافة ومصادرها بقدر ما يظل محكومًا بإطار تنظيمي آخر يمكن أن يفرض قيودًا إدارية واسعة على النشر والمنصات، بما يحد من القيمة الوقائية للاستثناء إذا تعارضت مقتضيات التنظيم الإعلامي مع مقتضيات حماية البيانات.

خلاصة الأمر أن مصر تمتلك قانونًا لحماية البيانات بمظهر معاصر، لكن معادلة الحماية تظل غير مستقرة طالما بقيت الاستثناءات الأمنية واسعة وقابلة للتمدد، وطالما ظل نموذج الإنفاذ قائمًا على تراخيص واعتمادات ومعايير يصوغها ويعتمدها مركز يُفترض أن يكون ضامنًا للحق. بالتالي تُذكر الخصوصية كحق، ثم تُفتح بوابات استثناء تجعل سقف الحماية النهائي مرتبطًا ببنية السلطة ومساراتها، لا بالمبادئ الحقوقية والقانونية وحدها.

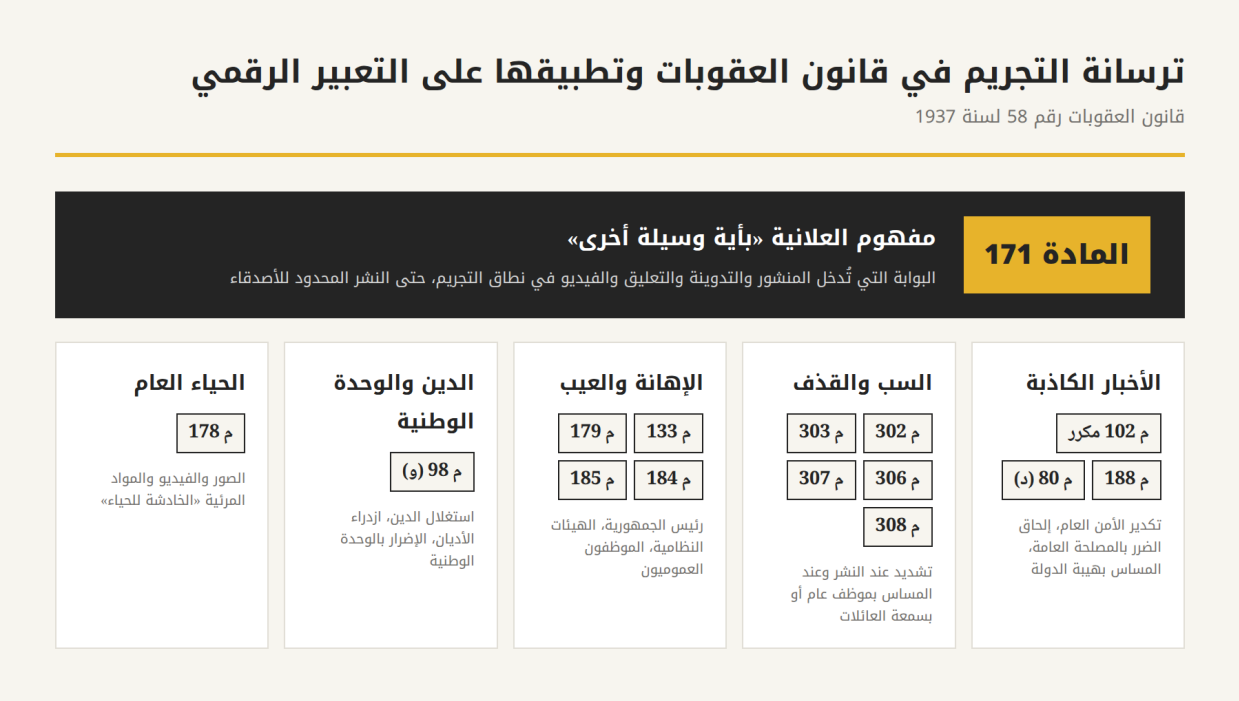
سابعًا: جرائم نشر الأخبار الكاذبة والسبّ والقذف كأدوات ضبط رقمي

يعمل قانون العقوبات المصري رقم 58 لسنة 1937، كأحد أكثر الأدوات فاعلية في تقييد الحقوق الرقمية اليوم. وتأتي من كونه مخزنًا واسعًا لصيغ تجريم مرنة قابلة لأن تُسقَط بسهولة على الكلام المنشور عبر الإنترنت.

وأبرز ما يفتح الباب لتطبيق هذه النصوص على التعبير عبر الإنترنت أن قانون العقوبات نفسه يضع تعريفًا واسعًا للعلانية والتحريض، يتضمن صراحةً فكرة النشر بأية وسيلة أخرى من وسائل العلانية، ويجعل الإسناد أو السب أو القذف أو التحريض إذا وقع بواسطة إحدى الطرق المبينة بالمادة 171 داخل نطاق التجريم.

تتحدث المادة 171 [37]عن التحريض العلني بالقول أو الصياح أو الفعل أو الإيماء، أو بالكتابة أو الرسوم أو الصور أو الرموز، أو بأية وسيلة أخرى من وسائل العلانية. هذا التوسع في مفهوم العلانية هو ما يجعل المنشور على منصة اجتماعية، أو تدوينة، أو تعليقًا، أو فيديو، قابلاً لأن يُعامل كنشر علني متى قُدِّر أنه وصل إلى الغير أو أتيح لهم الاطلاع عليه؛ حتى وإن كان نشرًا مخصصًا (محدود العلانية مثل النشر للأصدقاء فقط أو عبر جهات إتصال محددة) ومن هنا تبدأ ترسانة الجرائم التي تمس التعبير الرقمي داخل قانون العقوبات، وأشهرها جرائم الأخبار الكاذبة، وجرائم السب والقذف، وجرائم الإهانة أو العيب لهيئات الدولة أو موظفيها، إلى جانب جرائم ذات صلة بالمعتقد أو الدين أو التحريض على الكراهية والتمييز، وجرائم "النشر المخِل بالحياء".

[37] المادة 171 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"كل من حرض واحداً أو أكثر بارتكاب جناية أو جنحة بقول أو صياح جهر به علناً أو بفعل أو إيماء صدر منه علناً أو بكتابة أو رسوم أو صور أو صور شمسية أو رموز أو أية طريقة أخرى من طرق التمثيل جعلها علنية أو بأية وسيلة أخرى من وسائل العلانية يعد شريكاً في فعلها ويعاقب بالعقاب المقرر لها إذا ترتب على هذا التحريض وقوع تلك الجناية أو الجنحة بالفعل.
أما إذا ترتب على التحريض مجرد الشروع في الجريمة فيطبق القاضي الأحكام القانونية في العقاب على الشروع.
ويعتبر القول أو الصياح علنياً إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريق اللاسلكي أو بأية طريقة أخرى.
ويكون الفعل أو الإيماء علنياً إذا وقع في محفل عام أو طريق عام أو في أي مكان آخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان.
وتعتبر الكتابة والرسوم والصور والصور الشمسية والرموز وغيرها من طرق التمثيل علنية إذا وزعت بغير تمييز على عدد من الناس أو إذا عرضت بحيث يستطيع أن يراها من يكون في الطريق العام أو أي مكان مطروق أو إذا بيعت أو عرضت للبيع في أي مكان "



شكل (10): مواد قانون العقوبات المستخدمة في ملاحقة التعبير الرقمي

في محور نشر الأخبار الكاذبة، يتوزع التجريم على عدة مواد بحدود وظروف مختلفة. فالمادة 102 [38]مكرر تُعاقب كل من أذاع عمدًا أخبارًا أو بيانات أو إشاعات كاذبة إذا كان من شأن ذلك تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة، مع تشديد العقوبة في زمن الحرب.

ويمتد نطاق نشر الأخبار الكاذبة لتشمل حيازة محررات أو مطبوعات تتضمن تلك الأخبار الكاذبة إذا كانت معدّة للتوزيع أو لإطلاع الغير، وكذلك حيازة وسائل الطبع أو التسجيل أو غيرها من وسائل العلانية المخصصة لطبع أو تسجيل أو إذاعة ذلك المحتوى.

وفي مستوى آخر، تركز المادة 188[39] على فعل النشر بسوء قصد لأخبار أو بيانات أو إشاعات كاذبة، أو أوراق مصطنعة أو مزورة، أو منسوبة كذبًا إلى الغير، إذا كان من شأن ذلك تكدير السلم العام أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة، وتقرر عقوبة الحبس والغرامة أو إحدى العقوبتين.

وبهذا يبرز منطق يتكرر كثيرًا في الممارسة، فليس مطلوبًا دائمًا أن يُحسم الكذب بمعيار معرفي صريح أو إجراءات تحقق محددة، بقدر ما يكفي-بحسب النص- توافر سوء القصد وأن يكون من شأن النشر إحداث أحد الآثار العامة التي يعددها القانون (كتكدير السلم العام أو الإضرار بالمصلحة العامة)، فنص المادة يضع ضوابط لا يمكن إثبات عكسها او دحضها مثل أن نشر الخبر أو البيان كان بسوء قصد وهو أمر تقديري يصعب إثباته.

[38] المادة 102 مكرر من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب بالحبس وبغرامة لا تقل عن خمسين جنيهاً ولا تجاوز مائتي جنيه كل من أذاع عمداً أخباراً أو بيانات أو إشاعات كاذبة إذا كان من شأن ذلك تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة.
وتكون العقوبة السجن وغرامة لا تقل عن مائة جنيه ولا تجاوز خمسمائة جنيه إذا وقعت الجريمة في زمن الحرب.
ويعاقب بالعقوبات المنصوص عليها في الفقرة الأولى كل من حاز بالذات أو بالواسطة أو أحرز محررات أو مطبوعات تتضمن شيئاً مما نص عليه في الفقرة المذكورة إذا كانت معدة للتوزيع أو لاطلاع الغير عليها، وكل من حاز أو أحرز أية وسيلة من وسائل الطبع أو التسجيل أو العلانية مخصصة ولو بصفة وقتية لطبع أو تسجيل أو إذاعة شيء مما ذكر."
[39] المادة 188 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
" يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألف جنيه أو بإحدى هاتين العقوبتين كل من نشر بسوء قصد بإحدى الطرق المتقدم ذكرها أخباراً أو بيانات أو إشاعات كاذبة أو أوراقاً مصطنعة أو مزورة أو منسوبة كذباً إلى الغير، إذا كان من شأن ذلك تكدير السلم العام أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة"

وعلى خط أكثر اتصالًا بصورة الدولة خارجيًا تُجرّم المادة 80 (د)[40] إذاعة أخبار أو بيانات أو إشاعات كاذبة في الخارج حول الأوضاع الداخلية للبلاد إذا كان من شأنها إضعاف الثقة المالية بالدولة أو هيبتها واعتبارها أو الإضرار بالمصالح القومية، مع تشديد في زمن الحرب.

وبما أن الإنترنت بطبيعته عابر للحدود، فإن قابلية تداول المحتوى عالميًا تُدخل -من حيث الإمكان- المنشورات المتاحة خارج الإقليم ضمن مجال النقاش حول تطبيق هذا النص، بحسب ما تراه جهات التحقيق من انطباق عناصره على واقعة بعينها.

وفي محور السب والقذف كجرائم تمس حرية التعبير على الإنترنت خصوصًا حين يكون التعبير سياسيًا أو صحفيًا أو نقدًا عامًا، يعرّف قانون العقوبات القذف في المادة 302[41] بأنه إسناد أمور للغير بواسطة إحدى الطرق المبينة بالمادة 171، أي أمور لو كانت حقيقية لأوجبت عقاب من أسندت إليه قانونياً أو احتقاره عند أهل وطنه؛ وبالتالي يمكن استخدام هذا النص في حالة النشر عبر الإنترنت باعتباره شكلاً من أشكال العلانية.

ثم تأتي المادة 303[42] لتحدد عقوبة القذف بالغرامة ضمن حدود معينة، مع تغليظ إذا وقع القذف في حق موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة بسبب أداء الوظيفة أو النيابة أو الخدمة العامة. وبالتوازي، تعرّف المادة 306[43] السب بأنه كل سب لا يشتمل على إسناد - الفعل الذي بناء عليه نشأت الجريمة - واقعة معينة بل يتضمن خدشًا للشرف أو الاعتبار، ويعاقب عليه -عند توافر العلانية وفق المادة 171- بغرامة ضمن حدودها.

ولا يقف الأمر عند النشر من قبل الأفراد (ليست مؤسسة صحفية)، لأن القانون يضع آليات تشديد مرتبطة بطريق النشر، فالمادة 307 تقرر أنه إذا ارتُكبت جرائم معينة (منها المواد 182 إلى 185 و303 و306) بطريق النشر في إحدى الجرائد أو المطبوعات تُرفع الحدود الدنيا والقصوى للغرامات إلى ضعفيها، وهو منطق يجعل "النشر العام" عاملًا مُشدِّدًا في ذاته. ثم تأتي المادة 308 لتشدد أكثر إذا تضمن العيب أو الإهانة أو القذف أو السب طعنًا في عرض الأفراد أو خدشًا لسمعة العائلات، فتجعل العقوبة الحبس والغرامة معًا وفق الحدود التي يقررها النص، وتضع حدًا أدنى للحبس والغرامة في حالة النشر في الجرائد أو المطبوعات.

وفي القضايا المتعلقة بالإهانة أو العيب المتصل بالدولة ومؤسساتها أو موظفيها -وهو محور يتقاطع كثيرًا مع التعبير السياسي على الإنترنت- تظهر مجموعة مواد تُجرّم أنماطًا من الإهانة أو السب إذا تعلقت بموظف عام أو هيئة عامة أو رأس الدولة. وهو ما يمكن

---

[40] المادة 80 (د) من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على خمس سنوات وبغرامة لا تقل عن 100 جنيه ولا تجاوز 500 جنيه أو بإحدى هاتين العقوبتين كل مصري أذاع عمداً في الخارج أخباراً أو بيانات أو إشاعات كاذبة حول الأوضاع الداخلية للبلاد وكان من شأن ذلك إضعاف الثقة المالية بالدولة أو هيبتها واعتبارها أو باشر بأية طريقة كانت نشاطاً من شأنه الإضرار بالمصالح القومية للبلاد.
وتكون العقوبة السجن إذا وقعت الجريمة في زمن حرب "

[41] المادة 302 من قانون العقوبات المصري رقم رقم 58 لسنة 1937

"يعد قاذفاً كل من أسند لغيره بواسطة إحدى الطرق المبينة بالمادة 171 من هذا القانون أموراً لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانوناً أو أوجبت احتقاره عند أهل وطنه.
ومع ذلك فالطعن في أعمال موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة لا يدخل تحت حكم الفقرة السابقة إذا حصل بسلامة نية وكان لا يتعدى أعمال الوظيفة أو النيابة أو الخدمة العامة، وبشرط أن يثبت المتهم حقيقة كل فعل أسنده إلى المجني عليه، ولسلطة التحقيق أو المحكمة، بحسب الأحوال، أن تأمر بإلزام الجهات الإدارية بتقديم ما لديها من أوراق أو مستندات معززة لما يقدمه المتهم من أدلة لإثبات حقيقة تلك الأفعال.
ولا يقبل من القاذف إقامة الدليل لإثبات ما قذف به إلا في الحالة المبينة بالفقرة السابقة."

[42] المادة 303 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب على القذف بغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على خمسة عشر ألف جنيه.
فإذا وقع القذف في حق موظف عام أو شخص ذي صفة نيابية عامة أو مكلف بخدمة عامة، وكان ذلك بسبب أداء الوظيفة أو النيابة أو الخدمة العامة، كانت العقوبة غرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على عشرين ألف جنيه"

[43] المادة 306 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأي وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب عليه في الأحوال المبينة بالمادة 171 بغرامة لا تقل عن ألفي جنيه ولا تزيد على عشرة آلاف جنيه"

أن يترتب عليه توقيع عقوبة سالبة للحرية على خلفية النشر، بالإضافة إلى إحتمالات التوسع في الاتهامات في حالة وجود انتقادات سياسية. فالمادة 133[44] تعاقب من أهان بالإشارة أو القول أو التهديد موظفًا عموميًا أو أحد رجال الضبط أو أي مكلف بخدمة عمومية أثناء تأدية وظيفته أو بسببها، وتغلظ العقوبة إذا وقعت الإهانة على محكمة أو مجلس أثناء انعقاد الجلسة. كما تضع المادة 185[45] عقوبة خاصة لسبّ الموظف العام أو ذوي الصفة النيابية أو المكلف بخدمة عامة بسبب أداء الوظيفة أو النيابة أو الخدمة العامة.

وعلى مستوى آخر تنص المادة 179[46] على عقوبة إهانة رئيس الجمهورية بإحدى الطرق المتقدم ذكرها، أي عبر طرق العلانية، وهو ما يجعل المنشورات والتعليقات الرقمية داخلة في دائرة الإمكان التطبيقي متى اعتُبرت -وفق التكييف- إهانة. كما تعاقب المادة 184[47] من أهان أو سب مجلس الشعب/الشورى أو غيره من الهيئات النظامية أو الجيش أو المحاكم أو السلطات أو المصالح العامة بإحدى الطرق المتقدم ذكرها، بما يعني أن التعبير النقدي الحاد تجاه مؤسسات الدولة قد يُعاد توصيفه جنائيًا كإهانة أو سب بحسب تقدير جهة الاتهام أو المحكمة.

وفي محور التعبير المتصل بالدين أو العقيدة أو الجماعات، يضم قانون العقوبات نصوصًا تُستخدم لتجريم أشكال من الخطاب. فالمادة 98 (و)[48] تُعاقب من استغل الدين في الترويج بالقول أو بالكتابة أو بأية وسيلة أخرى لأفكار متطرفة بقصد إثارة الفتنة، أو تحقير/ازدراء أحد الأديان السماوية أو الطوائف المنتمية إليها، أو الإضرار بالوحدة الوطنية؛ وهي صياغة تجمع بين عنصر القصد وعنصر الوسيلة، ما يجعل فعل النشر على الانترنت قابل لتوجيه الاتهام متى قُدِّر توافر أركان جريمة المساس بالوحدة الوطنية، وبهذه الصياغة تصبح الوسيلة (الفضاء الرقمي) يصبح عرضة قابل لتطبيق العقوبات المتعلقة بجرائم إستغلال الأديان.

وفي القضايا المتعلقة بالنشر المخِل بالحياء الذي يطال محتوى الصور والفيديو والمواد المرئية المتداولة رقميًا تنص المادة 178[49] على تجريم نشر أو صنع أو حيازة بقصد الاتجار أو التوزيع أو العرض لمطبوعات أو مخطوطات أو رسومات أو صور أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عمومًا إذا كانت خادشة للحياء العام، بعقوبات الحبس والغرامة أو إحداهما.

44

المادة 133 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
من أهان بالإشارة أو القول أو التهديد موظفاً عموميا أو أحد رجال الضبط أو أي إنسان مكلف بخدمة عمومية أثناء تأدية وظيفته أو بسبب تأديتها يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تتجاوز مائتي جنيه مصري.
فإذا وقعت الإهانة على محكمة قضائية أو إدارية أو مجلس أو على أحد أعضائها وكان ذلك أثناء انعقاد الجلسة تكون العقوبة الحبس مدة لا تزيد على سنة أو غرامة لا تتجاوز خمسمائة جنيه مصري.

45 المادة 185 من قانون العقوبات المصري رقم رقم 58 لسنة 1937

"يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على عشرين ألف جنيه كل من سب موظفاً عاماً أو شخصاً ذا صفة نيابية عامة أو مكلفاً بخدمة عامة بسبب أداء الوظيفة أو النيابة أو الخدمة العامة، وذلك مع عدم الإخلال بتطبيق الفقرة الثانية من المادة 302 إذا وجد ارتباط بين السب وجريمة قذف ارتكبها ذات المتهم ضد نفس من وقعت عليه جريمة السب."

46 المادة 179 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على ثلاثين ألف جنيه كل من أهان رئيس الجمهورية بإحدى الطرق المتقدم ذكرها.

47 المادة 184 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب بالحبس وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من أهان أو سب بإحدى الطرق المتقدم ذكرها مجلس النواب أو غيره من الهيئات النظامية أو الجيش أو المحاكم أو السلطات أو المصالح العامة."

48 المادة 98 (و) من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تجاوز خمس سنوات أو بغرامة لا تقل عن خمسمائة جنيه، ولا تجاوز ألف جنيه كل من استغل الدين في الترويج بالقول أو بالكتابة أو بأية وسيلة أخرى لأفكار متطرفة بقصد إثارة الفتنة أو تحقير أو ازدراء أحد الأديان السماوية أو الطوائف المنتمية إليها أو الإضرار بالوحدة الوطنية"

49 المادة 178 من قانون العقوبات المصري رقم رقم 58 لسنة 1937
"يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من نشر أو صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صوراً محفورة أو منقوشة أو رسوماً يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت خادشة للحياء العام"

ثامنًا: السيطرة القانونية على منتجي المحتوى الرقمي عبر "إعادة التصنيف" و"التجريم الأخلاقي"

تعمل السيطرة القانونية على منتجي المحتوى الرقمي في مصر عبر مسارين متوازيين يتقاطعان في النتيجة وإن اختلفا في الأدوات. المسار الأول تنظيمي/إداري يعيد تصنيف الحسابات المؤثرة بوصفها وسائل نشر خاضعة لولاية تنظيمية شبيهة بالإعلام التقليدي. والمسار الثاني جنائي يوسع نطاق التجريم ليطال أنماطًا من التعبير الرقمي تحت عناوين أخلاقية واجتماعية فضفاضة. والجمع بين المسارين يضع صانع المحتوى بين منطق الامتثال التنظيمي الذي يهدد بالوقف/الحجب، ومنطق الاشتباه الجنائي الذي يفتح الباب للحبس والغرامة.

أولًا: إعادة التصنيف وإخضاع صانع المحتوى لولاية تنظيمية شبيهة بالإعلام التقليدي

لا يكتفي قانون تنظيم الصحافة والإعلام بإدارة المؤسسات الصحفية والإعلامية بوصفها كيانات مهنية، بل يمد أثره إلى الفضاء الرقمي الشخصي عبر معيار حجم الجمهور. فالمادة (19)[50] لا تضع محظورات على الصحف والوسائل والمواقع فقط، وإنما تُلزم المواقع والمدونات والحسابات الشخصية بذات المحظورات متى بلغ عدد المتابعين خمسة آلاف أو أكثر.

وبالتالي فإن محتوى الحساب الشخصي لا يعود مجرد تعبير فردي، بل يُعامل قانونيًا كوسيط نشر عام، ويُفترض فيه الامتثال لمعايير تنظيمية صيغت أصلًا لقطاع الصحافة والإعلام. وتزداد حدة هذا التحول لأن النص لا يكتفي بتقرير الالتزام، بل يفرض على المجلس الأعلى اتخاذ الإجراء المناسب ويمنحه سلطة وقف أو حجب الموقع/المدونة/الحساب بقرار منه، مع فتح باب الطعن أمام القضاء الإداري.

عمليًا يؤدي ذلك إلى أن يدخل صانع المحتوى في علاقة تنظيمية مع جهة إدارية، لا لأن نشاطه اتخذ شكلًا مؤسسيًا أو مهنيًا، بل لأن جمهوره اتسع. وفي هذا النموذج تصبح ممارسات (مثل السخرية، التجريب، اللغة غير الرسمية، التعليق السريع) أكثر حساسية؛ لأن معيار المخالفة في المادة (19) واسع (أخبار كاذبة، تحريض، كراهية، تمييز... إلخ) ويُفعَّل عبر قرار إداري سريع الأثر.

هذا لا يعني أن الطعن غير متاح، فهو متاح بالفعل، لكنه يعني أن التدخل يقع أولًا ثم يُراجع لاحقًا، وهو ترتيب يزيد الميل إلى امتثال وقائي لدى المبدعين والمؤثرين، حيث تُقدَّم سلامة الحساب واستمرارية الوصول للجمهور على مساحة حرية التعبير.

[50] المادة 19: يحظر على الصحيفة أو الوسيلة الإعلامية أو الموقع الإلكتروني نشر أو بث أخبار كاذبة، أو ما يدعو أو يحرض على مخالفة القانون أو إلى العنف أو الكراهية، أو ينطوي على تمييز بين المواطنين، أو يدعو إلى العنصرية أو يتضمن طعنا في أعراض الأفراد، أو سبا أو قذفا لهم، أو امتهانا للأديان السماوية أو للعقائد الدينية.
ويلتزم بأحكام الفقرة السابقة كل موقع إلكتروني شخصي أو مدونة إلكترونية شخصية أو حساب إلكتروني شخصي، يبلغ عدد متابعيه خمسة آلاف متابع أو أكثر.
ومع عدم الإخلال بالمسئولية القانونية المترتبة على مخالفة أحكام هذه المادة، يجب على المجلس الأعلى اتخاذ الإجراء المناسب حيال المخالفة، وله في سبيل ذلك وقف أو حجب الموقع أو المدونة أو الحساب المشار إليه بقرار منه. ولذوي الشأن الطعن على القرار الصادر بذلك أمام محكمة القضاء الإداري.

ثانيًا: التجريم الأخلاقي والاجتماعي كمسار جنائي يطارد التعبير الشخصي

على مسار موازٍ، يقدّم قانون مكافحة جرائم تقنية المعلومات طبقة مختلفة من السيطرة لا تقوم على إعادة تصنيف صانع المحتوى كفاعل تنظيمي، بل على تحويله إلى مشتبه به جنائي عبر نصوص تتدخل في الهوية الرقمية وأنماط السلوك والتعبير. وتظهر هنا المادتان (24) و(25) كنقطتي ارتكاز[51].

المادة (24) تجرّم اصطناع بريد أو موقع أو حساب ونسبته زورًا للغير، مع عقوبات تتدرج وتشتد إذا ترتب على الاستخدام إساءة لمن نُسب إليه الحساب أو إذا كانت الجريمة واقعة على جهة عامة. [52]

من حيث المبدأ، يحقق هذا التجريم حماية من انتحال الهوية والابتزاز. غير أن الإشكال يظهر عندما تتحول حدود الاصطناع في التطبيق إلى مساحة تؤثر على ممارسات رقمية واسعة مثل الحسابات الساخرة أو الأسماء المستعارة أو المحاكاة الساخرة، خصوصًا في بيئة يتداخل فيها النقد السياسي مع حساسية النظام العام.

وبالتالي لا يُفهم الخطر فقط كخطر على السمعة الفردية، بل كضغط على حق الظهور بأشكال متعددة في الفضاء الرقمي، بما يضيق المجال أمام أساليب تعبير قائمة على التخفي أو السخرية أو تقنيات الشخصية الرقمية التي لا تطابق الاسم الرسمي.

أما المادة (25) فتُنتج نموذجًا أكثر تعقيدًا لأنها تجمع في مادة واحدة بين عناوين متباينة مثل الاعتداء على قيم الأسرة من جهة، وصور متعددة من انتهاك الخصوصية والمضايقة الرقمية والترويج دون موافقة من جهة أخرى، مع عقوبة حبس وغرامة.

هذا الجمع يخلق أثرين متداخلين:

- الأول أن مفهوم قيم الأسرة يظل معيارًا واسعًا بطبيعته، قابلًا للتمدد في التفسير، بما يجعل التجريم الأخلاقي قابلًا للانتقال من حماية أشخاص من ضرر محدد إلى ضبط أنماط تعبير واختيار شخصي.
- الثاني أن المادة لا تُفصل بوضوح بين الضرر المحدد (انتهاك خصوصية شخص بعينه/مضايقة مباشرة) وبين التقييم القيمي للمحتوى، فتتجاور الأفعال غير المتجانسة داخل قالب عقابي واحد.

---

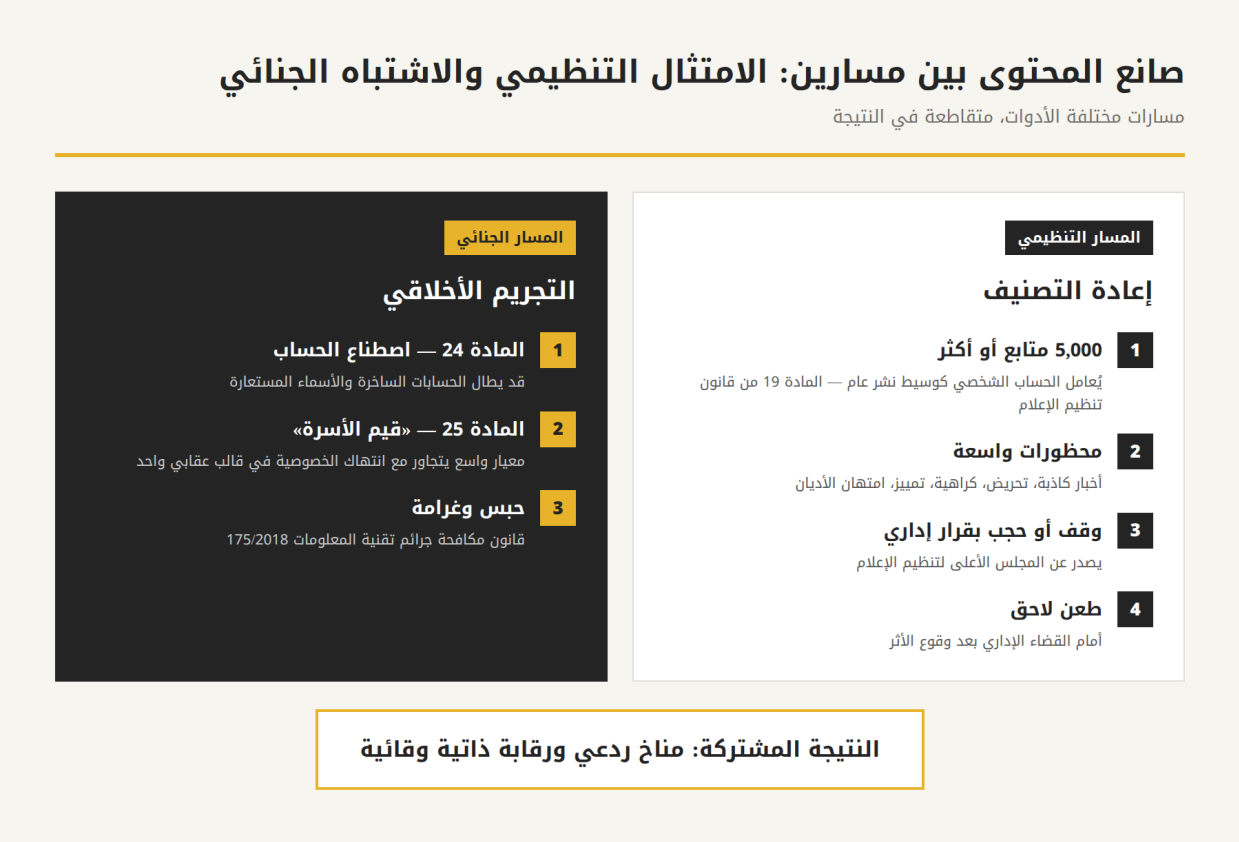
[51] المادة (24) الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني
يعاقب بالحبس مدة لا تقل عن 3 أشهر وغرامة لا تقل عن 10 آلاف جنيه ولا تجاوز 30 ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدا إلكترونيا أو موقعا أو حاسبًا خاصًا ونسبه زورا لشخص طبيعي أو اعتبارى.
فإذا استخدم الجانى البريد أو الموقع أو الحساب الخاص المصطنع فى أمر يسئ إلى من نسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة وغرامة لا تقل عن 50 ألف جنيه ولا تجاوز 200 ألف جنيه أو بإحدى العقوبتين.
وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة فتكون العقوبة السجن والغرامة التى لا تقل عن 100 ألف جنيه ولا تزيد على 300 ألف جنيه.

المادة (25) الجرائم المتعلقة بالاعتداء على حرمه الحياة الخاصة والمحتوى المعلوماتى غير المشروع
يعاقب بالحبس مدة لاتقل عن ستة أشهر، وبغرامة لاتقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو باحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الاسرية فى المجتمع المصرى، أو انتهك حرمة الحياه الخاصة أو ارسل بكثافة العديد من الرسائل الاليكترونية لشخص معين دون موافقته، أو منح بيانات إلى نظام أو موقع اليكترونى لترويج السلع أو الخدمات دون موافقته أو بالقيام بالنشر عن طريق الشبكة المعلوماتية أو باحدى وسائل تقنية المعلومات، لمعلومات أو اخبار أو صور وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة ام غير صحيحة.

[52] جريمة اصطناع الحسابات وعلاقتها بالحسابات الساخرة والحسابات المزيفة ، مؤسسة مسار، مايو 2021، الرابط: https://masaar.net/ar/%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9-%D8%A7%D9%84%D8%AD%D8%B3%D8%A7%D8%A8%D8%A7%D8%AA-%D9%88%D8%B9%D9%84%D8%A7%D9%82%D8%AA%D9%87%D8%A7-%D8%A8%D8%A7%D9%84%D8%AD%D8%B3/

وتدعم قراءات مسار لهذه المادة فكرة أن الصياغة الملتبسة -وخاصة عبارة الاعتداء على قيم الأسرة -تفتح مساحة واسعة للتوسع في الاتهام، بما يضعف قابلية التوقع ويؤثر على مبدأ الشرعية الجنائية. وهو ما تم توثيقه من منظمات المجتمع المدني المصري حول استخدام المادة (25) بوصفها عنوانًا لنمط ملاحقات توسع التجريم لأفعال لم تكن مجرّمة خارج الإنترنت في أغلب الأحوال، وتقرأها كأداة للضبط الاجتماعي بآثار طبقية وجندرية.[53]

ويُنتج الجمع بين المسارين السابقين (إعادة التصنيف والتجريم الأخلاقي) وضعًا مزدوجاً من الضغط على منتجي المحتوى. من جهة، يُدفعون إلى امتثال تنظيمي لأن حساباتهم قد تُعامل كوسيلة نشر قابلة للوقف أو الحجب إداريًا عند محظورات واسعة. ومن جهة أخرى، يواجهون مسارًا جنائيًا يمكن أن يطاول أساليب الظهور والتعبير عبر عناوين أخلاقية واجتماعية فضفاضة أو عبر تجريم بعض صور بناء الهوية الرقمية.



شكل (11): المساران التنظيمي والجنائي في مواجهة صناع المحتوى

وذلك لا يؤدي فقط إلى ملاحقات وعقوبات، بل إلى مناخ ردعي يدفع إلى رقابة ذاتية، ويعيد تشكيل المجال العام الرقمي بحيث يصبح الأكثر انتشارًا أو الأكثر اختلافًا اجتماعيًا هم الأكثر تعرضًا للتنظيم الإداري وللتجريم الأخلاقي.

[53] تأديب المجتمع: الملاحقة القانونية برعاية "قيم الأسرة المصرية"، المبادرة المصرية للحقوق الشخصية، ديسمبر 2025، الرابط: https://eipr.org/publications/%D8%AA%D8%A3%D8%AF%D9%8A%D8%A8-%D8%A7%D9%84%D9%85%D8%AC%D8%AA%D9%85%D8%B9-%D8%A7%D9%84%D9%85%D9%84%D8%A7%D8%AD%D9%82%D8%A9-%D8%A7%D9%84%D9%82%D8%A7%D9%86%D9%88%D9%86%D9%8A%D8%A9-%D8%A8%D8%B1%D8%B9%D8%A7%D9%8A%D8%A9-%D9%82%D9%8A%D9%85-%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A%D8%A9

تاسعًا: مكافحة الإرهاب.. التشريع الذي يُحوّل الإنترنت إلى مساحة اشتباه دائمة

لا يمكن توصيف أوضاع الحقوق الرقمية في مصر بدقة دون وضع قانون مكافحة الإرهاب رقم 94 لسنة 2015 في مركز الصورة. هذا القانون لا يعمل فقط بوصفه إطارًا عقابيًا لمواجهة عنف مسلح، بل بوصفه قراءة تشريعية تُعيد تعريف الفضاء الرقمي كله باعتباره مجالًا أمنيًا، تُدار فيه حرية التعبير وتداول المعلومات والخصوصية باعتبارها عناصر قابلة للتعليق عند أول استدعاء لمصطلحات الأمن القومي والإرهاب.

«تصبح الحقيقة مسألة قرار إداري أكثر من كونها ثمرة تحقيق مستقل»

يبدأ هذا الأثر من طريقة تعريف الإرهاب والأفعال الإرهابية على نحو واسع يسمح بالتمدد إلى ما يتجاوز العنف المباشر وهو ما نظمته المادة رقم 2[54] من القانون. فالمادة لا تقتصر على التعريف التقليدي لمفهوم الإرهاب والذي يتعلق بصور العنف المسلح، بل تُدخِل ضمنه كل استخدام عبارات مثل التهديد او الترويع بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر أو إيذاء الأشخاص أو إلقاء الرعب بينهم أو المساس بالحقوق والحريات، والتعريف في صيغته هذه يشمل مصطلحات عامة يتعذر قانونًا ضبطها ومعرفة أبعادها والسلوك او الفعل الذي يُرتب حدوثها. وداخل المجال الرقمي، يتجسد هذا الاتساع في مسارين متلازمين:

- المسار الأول هو تجريم الترويج والدعاية بوصفهما مدخلًا مباشرًا إلى ملاحقة المحتوى. فالمادة 28[55] تجرّم الترويج المباشر وغير المباشر لأفكار أو أنشطة إرهابية عبر الكتابة أو الخطابة أو النشر أو البث. هذه الصياغات تُدخل التعبير

[54] المادة 2 من قانون مكافحة الإرهاب رقم 94 لسنة 2015

في تطبيق أحكام هذا القانون، يقصد بالألفاظ والعبارات التالية المعنى المبين قرين كل منها:
(أ) الجماعة الإرهابية: كل جماعة أو جمعية أو هيئة أو منظمة أو عصابة مؤلفة من ثلاثة أشخاص على الأقل أو غيرها أو كيان تثبت له هذه الصفة، أياً كان شكلها القانوني أو الواقعي سواء كانت داخل البلاد أو خارجها، وأياً كان جنسيتها أو جنسية من ينتسب إليها، تهدف إلى ارتكاب واحدة أو أكثر من جرائم الإرهاب أو كان الإرهاب من الوسائل التي تستخدمها لتحقيق أو تنفيذ أغراضها الإجرامية.
(ب) الإرهابي: كل شخص طبيعي يرتكب أو يشرع في ارتكاب أو يحرض أو يهدد أو يخطط في الداخل أو الخارج لجريمة إرهابية بأية وسيلة كانت، ولو بشكل منفرد، أو يساهم في هذه الجريمة في إطار مشروع إجرامي مشترك، أو تولى قيادة أو زعامة أو إدارة أو إنشاء أو تأسيس أو اشترك في عضوية أي من الكيانات الإرهابية المنصوص عليها في المادة رقم (1) من قرار رئيس جمهورية مصر العربية بالقانون رقم 8 لسنة 2015 في شأن تنظيم قوائم الكيانات الإرهابية والإرهابيين أو يقوم بتمويلها، أو يساهم في نشاطها مع علمه بذلك.
(ج) الجريمة الإرهابية: كل جريمة منصوص عليها في هذا القانون، وكذا كل جناية أو جنحة ترتكب باستخدام إحدى وسائل الإرهاب أو بقصد تحقيق أو تنفيذ غرض إرهابي، أو بقصد الدعوة إلى ارتكاب أية جريمة مما تقدم أو التهديد بها، وذلك دون إخلال بأحكام قانون العقوبات.
(د) الأسلحة التقليدية: الأسلحة والذخائر والمفرقعات والمواد الجيلاتينية المنصوص عليها قانوناً.
(هـ) الأسلحة غير التقليدية: الأسلحة والمواد النووية والكيماوية والبيولوجية والإشعاعية والجرثومية، أو أية مواد أخرى طبيعية أو اصطناعية، صلبة أو سائلة، أو غازية أو بخارية، أياً كان مصدرها أو طريقة إنتاجها، لها القدرة والصلاحية على إزهاق الأرواح أو إحداث إصابات بدنية أو نفسية خطيرة بها، أو إلحاق الضرر بالبيئة أو بالمباني والمنشآت.
(و) الأموال أو الأصول: جميع الأصول المادية والافتراضية وعائداتها والموارد الاقتصادية، ومنها النفط والموارد الطبيعية الأخرى أو الممتلكات أيا كان نوعها، سواء كانت مادية أو معنوية، منقولة أو ثابتة، بما في ذلك المستندات والعملات الوطنية أو الأجنبية، والأوراق المالية أو التجارية والصكوك والمحررات المثبتة لكل ما تقدم أيا كان شكلها، بما في ذلك الشكل الرقمي أو الإلكتروني والائتمان المصرفي والشيكات المصرفية والاعتمادات المستندية، وأي فوائد أو أرباح أو مصادر دخل ترتبت على هذه الأموال أو الأصول أو تولدت عنها، أو أي أصول أخرى أعدت لاستخدامها في الحصول على تمويل أو منتجات أو خدمات وجميع الحقوق المتعلقة بأي منها. كما تشمل الأصول الافتراضية التي لها قيمة رقمية يمكن تداولها أو نقلها أو تحويلها لشكل رقمي وتستخدم كأداة للدفع أو للاستثمار.

[55] المادة 28 من قانون مكافحة الإرهاب رقم 94 لسنة 2015

ضمن منظومة اشتباه، خصوصًا في سياق مصري تتوسع فيه تهمة الترويج لتشمل نقل معلومات أو تحليل سياسات أو حتى نشر شهادات تتعارض مع الرواية الرسمية. وهذا النوع من التجريم لا يحتاج أن يثبت وقوع عمل عنيف، بل يكفي أن يُقال إن المحتوى يخلق مناخًا أو تعاطفًا أو يبرر فعلًا، وهي منطقة رمادية تتضخم فيها سلطة التأويل على حساب حرية التعبير.

- المسار الثاني هو تقييد النشر الصحفي وتثبيت الرواية الرسمية عبر أدوات عقابية. قانون مكافحة الإرهاب وخاصة المادة 35[56] يتضمن أحكامًا تُعاقب على نشر معلومات عن العمليات الإرهابية تخالف البيانات الرسمية الصادرة عن الدولة، وهي نقطة شديدة الحساسية لأنها تجعل الحقيقة مسألة قرار إداري أكثر من كونها ثمرة تحقيق مستقل. فالنتيجة العملية هي تضييق الصحافة الاستقصائية، وتجريم التغطية التي تعتمد على شهود أو مصادر غير رسمية، وإنتاج ردع يجعل غرف الأخبار تتجنب الاقتراب من ملفات أمنية، وهو ما ينعكس مباشرة على حق الجمهور في المعرفة وعلى قدرة المجتمع المدني على الرصد والتحقق.

الزاوية الأشد اتصالًا بالحقوق الرقمية هي أن قوانين مكافحة الإرهاب تفتح مساحة واسعة لإجراءات تقييدية ذات طابع إداري مع رقابة محدودة، مثل المنع من السفر، والمراقبة، وتقييد الاتصالات، والملاحقة أمام نيابات متخصصة، وهي إجراءات تزيد قدرتها على التأثير في المجال الرقمي لأنها تعمل بسرعة وبسقف منخفض من الضوابط الإجرائية.

"يُعاقب بالسجن مدة لا تقل عن خمس سنين كل من روج أو أعد للترويج، بطريق مباشر أو غير مباشر، لارتكاب أية جريمة إرهابية سواء بالقول أو الكتابة أو بأية وسيلة أخرى. ويُعد من قبيل الترويج غير المباشر، الترويج للأفكار والمعتقدات الداعية لاستخدام العنف. وذلك بأي من الوسائل المنصوص عليها في الفقرة السابقة من هذه المادة. وتكون العقوبة السجن مدة لا تقل عن سبع سنين، إذا كان الترويج داخل دور العبادة، أو بين أفراد القوات المسلحة، أو قوات الشرطة، أو في الأماكن الخاصة بهذه القوات. ويُعاقب بذات العقوبة المقررة في الفقرة الأولى من هذه المادة كل من حاز أو أحرز أية وسيلة من وسائل الطبع أو التسجيل أو العلانية استعملت أو أعدت للاستعمال، ولو بصفة وقتية، بقصد طبع أو تسجيل أو إذاعة شيء مما ذكر "

[56] المادة 35 من قانون مكافحة الإرهاب رقم 94 لسنة 2015

"يُعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز خمسمائة ألف جنيه كل من تعمد، بأية وسيلة كانت، نشر أو إذاعة أو عرض أو ترويج أخبار أو بيانات غير حقيقية عن أعمال إرهابية وقعت داخل البلاد، أو عن العمليات المرتبطة بمكافحتها بما يخالف البيانات الرسمية الصادرة عن وزارة الدفاع، وذلك كله دون إخلال بالعقوبات التأديبية المقررة. وفي الأحوال التي ترتكب فيها الجريمة بواسطة شخص اعتباري، يُعاقب المسئول عن الإدارة الفعلية لهذا الشخص بذات العقوبة المقررة في الفقرة الأولى من هذه المادة ما دامت الجريمة قد ارتكبت لحسابه أو لمصلحته، ويكون الشخص الاعتباري مسئولاً بالتضامن عما يحكم به من غرامات وتعويضات. وفي جميع الأحوال، للمحكمة أن تقضي بمنع المحكوم عليه من مزاولة المهنة لمدة لا تزيد على سنة، إذا وقعت الجريمة إخلالاً بأصول مهنته"

عاشرًا: العدالة الإجرائية في القضايا الرقمية

أُقِرَّت التعديلات على قانون الإجراءات الجنائية الجديد في مصر بموجب القانون رقم 174 لسنة 2025، مع تعديلات جوهرية على مواد كانت محل اعتراض رئاسي، ثم نُشر القانون بالجريدة الرسمية في 12 نوفمبر 2025، وكان من المقرر بدء العمل به في 1 أكتوبر 2026، قبل أن يوافق مجلس النواب في 30 سبتمبر 2026 على ارجاء تطبيقه لمدة عام ليبدأ العمل به في أكتوبر 2027.

وتشمل التعديلات، محاور جوهرية تغيّر بشكل أو بآخر بالمفاهيم الإجرائية المستقرة، وفي حقيقة الأمر تأتي هذه التعديلات لتقنن ممارسات جديدة اعتادت عليها السلطات وجهات إنفاذ القانون في مصر خلال السنوات الأخيرة، ويمكن أن نبرز أهم التعديلات ذات الصلة بالحقوق الرقمية في النقاط التالية:



شكل (12): مواد قانون الإجراءات الجنائية الجديد ذات الصلة بالحقوق الرقمية

أولًا: مراقبة الاتصالات والمحتوى الرقمي

تقوم المادة (117)[57] من قانون الإجراءات الجنائية بنقل المراقبة من نطاق التنصت بالمعنى الضيق، أي التنصت على المكالمات الصوتية إلى نطاق رقمي واسع ومفصل من خلال مراقبة وسائل التواصل الإجتماعي والبريد الإلكتروني والرسائل النصية والصوتية

[57] مادة (117) من القانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"يكون لأعضاء النيابة العامة من درجة رئيس نيابة على الأقل في تحقيق الجنايات المنصوص عليها في الأبواب الأول والثاني والثالث والرابع من الكتاب الثاني من قانون العقوبات، بالإضافة إلى الاختصاصات المقررة للنيابة العامة، سلطة إصدار أمر مُسبب لمدة لا تزيد على ثلاثين يومًا، بضبط الخطابات والرسائل والبرقيات والجرائد والمطبوعات والطرود، وبمراقبة الاتصالات السلكية واللاسلكية، وحسابات مواقع التواصل الاجتماعي ومحتوياتها المختلفة غير المتاحة للجميع، والبريد الإلكتروني، والرسائل النصية أو المسموعة أو المصورة على الهواتف والأجهزة وأي وسيلة تقنية أخرى، وضبط الوسائط الحاوية لها، أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة.

ويجوز تجديد الأمر المشار إليه في الفقرة الأولى من هذه المادة مدة أو مددًا أخرى مماثلة.

المخزنة على الأجهزة، لأنها تمنح أعضاء نيابة من درجة رئيس نيابة على الأقل سلطة إصدار أمر مسبب لمدة لا تزيد على ثلاثين يومًا، لا يقتصر على مراقبة الاتصالات السلكية واللاسلكية، بل يمتد صراحة إلى حسابات مواقع التواصل الاجتماعي ومحتوياتها المختلفة غير المتاحة للجميع، والبريد الإلكتروني، والرسائل النصية أو المسموعة أو المصورة على الهواتف والأجهزة وأي وسيلة تقنية أخرى، مع قابلية تجديد الأمر لمدد مماثلة.

المشكلة ليست وجود وسيلة للتحقيق، بل اتساع نطاق ما يمكن اعتراضه ومراقبته، بما يشمل بيانات واتصالات تحمل بطبيعتها أثرًا يتجاوز الشخص محل التحقيق إلى دوائر تواصله. كل توسع في المراقبة الرقمية يرفع كلفة المشاركة العامة والعمل الحقوقي والصحفي والنقابي لأن أثره الردعي لا يحتاج إلى إدانة؛ يكفي الإحساس بإمكانية الرصد.

ثانيًا: تحويل بدائل الحبس إلى منظومة تتبع رقمية

المادة 114[58] من قانون الإجراءات الجنائية أضافت ضمن تدابير بديلة للحبس الاحتياطي، "استخدام الوسائل التقنية في تتبع المتهم" مع إحالة تنظيمها إلى قرار من وزير العدل بالتنسيق مع وزيري الداخلية والاتصالات.

هذا النص يخلق خطرًا نوعيًا على الحريات الرقمية لأن التتبع التقني يعيد إنتاج القيد قبل الإدانة في صورة مراقبة لصيقة للحركة وربما للسلوك اليومي، ويحوّل المجال الخاص إلى مساحة امتثال قسري. التتبع ليس مجرد بديل أخف تلقائيًا؛ هو نقل للحرمان من الحرية من مكان الاحتجاز إلى البنية الرقمية: بيانات موقع، جداول حركة، وربما سجلات امتثال يمكن أن تُساء إدارتها أو تتوسع وظيفيًا خارج غرضها.

كما يكون لهؤلاء الأعضاء في تحقيق الجنايات المشار إليه في الفقرة الأولى من هذه المادة عدا الجنايات المنصوص عليها في الباب الثالث من الكتاب الثاني من قانون العقوبات، سلطة القاضي الجزئي فيما يتعلق بمدة الحبس الاحتياطي.

ويكون لهم فضلاً عن ذلك سلطة محكمة الجنح المستأنفة منعقدة في غرفة المشورة، المنصوص عليها في المادة 123 من هذا القانون، عند تحقيق الجرائم المنصوص عليها في الباب الأول والقسم الأول من الباب الثاني من الكتاب الثاني من قانون العقوبات بشرط ألا تزيد مدة الحبس في كل مرة على خمسة عشر يومًا"

[58] المادة 114 من قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية
"يجوز لعضو النيابة العامة في الأحوال المنصوص عليها بالمادة 113 من هذا القانون، وكذلك في الجنح الأخرى المعاقب عليها بالحبس أن يصدر بدلا من الحبس الاحتياطي أمرا مسببا بأحد التدابير الآتية:

1- إلزام المتهم بعدم مبارحة مسكنه أو موطنه.

2- إلزام المتهم بأن يقدم نفسه لمقر الشرطة في أوقات محددة.

3- حظر ارتياد المتهم أماكن محددة.

4- إلزام المتهم بعدم مغادرة نطاق جغرافي محدد إلا بعد الحصول على إذن

من النيابة العامة.

5- إلزام المتهم بالامتناع عن استقبال أو مقابلة أشخاص معينين أو الاتصال بهم بأي شكل من الأشكال.

6- منع المتهم مؤقتا من حيازة أو إحراز الأسلحة النارية وذخيرتها، وتسليمها لقسم أو مركز الشرطة الذي يقع في دائرته محل إقامته.

7- استخدام الوسائل التقنية في تتبع المتهم حال توافر ظروف العمل بها، ويصدر بها قرار من وزير العدل بالتنسيق مع وزيري الداخلية والاتصالات"

ثالثًا: القيود على الاتصال

المادة (114) من قانون الإجراءات الجنائية تضمنت تدبيرًا يفرض على المتهم الامتناع عن استقبال أو مقابلة أشخاص معينين أو الاتصال بهم بأي شكل من الأشكال، في البيئة الرقمية، عبارة بأي شكل تبتلع الهاتف والتطبيقات والمنصات والبريد الإلكتروني ورسائل الوسائط، وتخلق خطرًا مضاعفًا مثل توسع المنع ليصيب شبكات الدعم والعمل.

رابعًا: مراكز الإعلانات الهاتفية وربط الإجراءات بقاعدة بيانات الهواتف

تؤسس المادة (232)[59] من قانون الإجراءات الجنائية لمركز يتبع وزارة العدل للاستعلام عن الرقم القومي للمتهم ورقم الهاتف المحمول المثبت به وإرسال الإعلانات القضائية الخاصة بجلسات المحاكمة أو بالإنذارات القضائية الهاتفية والإلكترونية وإعداد تقرير بما يفيد استلام تلك الرسائل. والمادة (233)[60] تقرر صدور قرار تنظيمي لتحديد آلية إثبات تسلسل الإعلانات الهاتفية والإلكترونية وكيفية التحقق من وصولها.

هذه البنية تخلق مخاوف رقمية مباشرة لأن تشغيلها يعني إنشاء مسار حكومي دائم لتجميع بيانات اتصال وربطها بالرقم القومي داخل إجراءات جنائية. الخطر لا يقتصر على التسريب، بل يشمل التوسع الوظيفي، وتحوّل تقارير الاستلام إلى قرينة إجرائية قد تُنتج آثارًا جسيمة على حق الدفاع إذا استقر التطبيق على مساواة وصول الرسالة تقنيًا بعلم الشخص فعليًا، خصوصًا مع تفاوت السيطرة على الهاتف داخل الأسرة أو العمل، وتفاوت القدرة على الوصول الآمن للأجهزة والخدمات.

---

[59] مادة (232) من قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"ينشأ بدائرة كل محكمة جزئية مركز للإعلانات الهاتفية يتبع وزارة العدل يختص بالاستعلام من قطاع الأحوال المدنية عن الرقم القومي للمتهم ورقم الهاتف المحمول المثبت به، وفقًا للنظم والقواعد المعمول بها في قطاع الأحوال المدنية وبما لا يتعارض مع مقتضيات الأمن القومي وسرية قواعد البيانات القومية، وإرسال الإعلانات الهاتفية والإلكترونية وإعداد تقرير بما يفيد استلام تلك الرسائل.

ويقدر القاضي المختص الرسم المستحق على الإعلان الهاتفي وفقًا لحكم المادة 16 من القانون رقم 90 لسنة 1944 بشأن الرسوم القضائية ورسوم التوثيق في المواد المدنية، على أن يلزم بأدائه من يحكم عليه بالمصاريف الجنائية.

ويخصص الرسم المشار إليه بالفقرة الثانية من هذه المادة للإنفاق على تطوير مراكز الإعلان وإعداد قواعد البيانات اللازمة"

[60] مادة (233) من قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"يجب أن تشتمل الأوراق التي يقوم المحضرون بإعلانها على البيانات الآتية:

- تاريخ اليوم والشهر والسنة والساعة التي حصل فيها الإعلان.
- بيان القضية المعلن بشأنها، وموضوعها، وصفة المعلن إليه فيها.
- اسم المحضر والمحكمة التي يعمل بها.
- اسم المعلن إليه، ولقبه، ومهنته أو وظيفته، وموطنه فإن لم يكن موطنه معلومًا وقت الإعلان فآخر موطن كان له.
- تاريخ ومكان انعقاد الإجراء المعلن بشأنه.
- اسم وصفة من سلمت إليه صورة الورقة، وتوقيعه على الأصل بالاستلام.
- توقيع المحضر باسمه الثلاثي على كل من الأصل والصورة توقيعًا مقروءًا.

ويصدر قرار من وزير العدل، بالتنسيق مع الوزير المختص بتحديد آلية إثبات تسلسل الإعلانات الهاتفية والإلكترونية، وكيفية التحقق من وصولها."

وهنا تكمن المشكلة في أن أهمية الإعلان تتعلق بأن الهدف منه التأكيد على أن شخص المتهم على علم بالجلسات أو الإنذارات أو حتى طلب الحضور للنيابة، فلو تعاملنا على أن الشخص يفترض أنه علم بمجرد أنه استقبل الإعلان على هاتفه سوف يترتب على ذلك إشكاليات عديدة لأنه يتجاهل إشكاليات حول ملكية خط الهاتف وثبوت حيازته والتواجد داخل البلاد واحتمالات تغيير الخط وتعطل الهاتف، وهذه مشاكل إجرائية يتجاهلها القانون.

خامسًا: إجراءات التحقيق والمحاكمة عن بُعد

تضع المواد (530–537) من قانون الإجراءات الجنائية، ما يمكن وصفه بإطار التحقيق والمحاكمة عن بعد باستخدام وسائل الاتصال الحديثة المسموعة والمرئية. المادة (531)[61] تفتح الباب لاستخدام هذا المسار في إجراءات حساسة مثل النظر في أمر الحبس الاحتياطي والتدابير ومداهما والإفراج المؤقت واستئناف أوامرها.

والمادة (534)[62] تمنح جهات التحقيق والمحاكمة سلطة تسجيل وحفظ جميع الإجراءات التي تتم عن بعد وتفريغها في محاضر، مع ترتيب توقيعات رسمية دون توقيع المتهمين أو الشهود أو غيرهم على كل ورقة. ثم تأتي المادة (537)[63] لتربط تجهيز القاعات والأجهزة بتنسيق بين وزارتي العدل والداخلية وجهات أخرى.

الخطر هنا مرتبط بواقع أن الجلسة حين تصبح حدثًا رقميًا تكون السرية والعلانية وحقوق الدفاع مسألة بنية تشغيل، لتطرح مخاوف مثل من يتحكم في التسجيل والحفظ، ما حدود الوصول، ما مدة الاحتفاظ، وكيف تُدار الأعطال والانقطاعات. وجود النصوص لا يحسم الخطر ما لم تُبْنَ ضمانات تقنية وإجرائية تمنع أن يتحول التسجيل والحفظ إلى مصدر مراقبة إضافي أو أداة نزاع غير متكافئ على حقيقة ما جرى في الجلسة، فالدولة هي الحائزة والمسيطرة على ما يثبت ما حدث داخل الجلسات وحدها،

---

[61] مادة (531) من قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"يجوز لجهة التحقيق أو المحاكمة المختصة بحسب الأحوال اتخاذ كل أو بعض إجراءات التحقيق أو المحاكمة عن بُعد مع المتهمين، والشهود، والمجني عليهم، والخبراء، والمدعين بالحقوق المدنية، والمسئولين عنها، المنصوص عليها

في هذا القانون.

ويجوز لها اتخاذ تلك الإجراءات فيما يتعلق بالنظر في أمر الحبس الاحتياطي والتدابير ومدهما والإفراج المؤقت واستئناف أوامرها.

ولها بحسب الأحوال أن تقرر منع الكشف عن الشخصية الحقيقية للشهود بجميع وسائل وتقنيات الاتصال الحديثة المناسبة أثناء الإدلاء بأقوالهم، وذلك كُله مع مراعاة حكم المادة 525 من هذا القانون"

[62] مادة (534) قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"يكون لجهات التحقيق والمحاكمة المختصة أن تتخذ ما تراه مناسبًا لتسجيل وحفظ جميع الإجراءات التي تتم من خلال وسائل وتقنيات الاتصال الحديثة عن بعد، وتفريغها في محاضر، ولها أن تستعين بأحد الخبراء في ذلك، وتودع ملف القضية.

ويضع كل من عضو النيابة العامة أو قاضي التحقيق أو رئيس الدائرة والكاتب توقيعه على كل ورقة دون الحاجة إلى توقيع أي من المتهمين أو الشهود أو الخبراء

أو المترجمين أو أي توقيع آخر"

[63] مادة (537) قانون رقم 174 لسنة 2025 بإصدار قانون الإجراءات الجنائية

"تقوم وزارة العدل بالتعاون والتنسيق مع وزارة الداخلية والجهات والوزارات المعنية، بإعداد القاعات وأجهزة الاتصال المطلوبة لتنفيذ إجراءات التحقيق والمحاكمة عن بعد باستخدام وسائل وتقنيات الاتصال الحديثة في الجهات المختصة، وفي المؤسسات العقابية ومراكز الإصلاح والتأهيل، وغير ذلك من الإدارات ذات الصلة وتقديم المساعدة الفنية اللازمة لذلك."

وإذا حدثت مخالفة أثناء الجلسة من الدولة أو المحكمة سوف يطلب الدفاع من الدولة -التي هي خصم- أن توافق على إعطاءه نسخة من تسجيل بالجلسة بالأخطاء اللي حصلت.

حادي عشر: القواعد المنظمة لقطع الاتصالات

الإطار القانوني الأقدم الذي يفتح إمكان تعطيل الاتصالات بصورة مباشرة هو قانون تنظيم الاتصالات رقم 10 لسنة 2003. والأكثر التصاقًا بالمسألة ليس القطع كمصطلح أو قرار سياسي، بل السلطة التي تمنحها المادة 67[64] من القانون للسلطات المختصة كي تُخضع لإدارتها جميع خدمات وشبكات اتصالات أي مشغل أو مقدم خدمة، وأن تستدعي العاملين القائمين على التشغيل والصيانة، وذلك في حالات الكوارث أو التعبئة العامة، ثم تُضيف صياغة أوسع تسمح بالتدخل في "أي حالات أخرى تتعلق بالأمن القومي".

هذه الصياغة تُنشئ من الناحية العملية سلطة على مستوى البنية التحتية، لا على مستوى المحتوى. فهي لا تتحدث فقط عن إيقاف خدمة بعينها، وإنما عن نقل إدارة الشبكة وخدماتها إلى يد الدولة عند تحقق الحالات المشار إليها.

وتنبع خطورة المادة 67 من عنصرين متلازمين. الأول هو غموض المصطلحات الحاكمة، خصوصًا تعبير "السلطات المختصة" ومعيار "أي حالات أخرى تتعلق بالأمن القومي"، وهما معياران لا يضع لهما القانون عتبة إثبات أو تعريفًا تشغيليًا يحد من قابلية التمدد.

والثاني هو أن النص لا يضع، في ذاته، شروطًا تفصيلية تتصل بمدة التدخل، أو نطاقه الجغرافي، أو درجة التناسب بين الخطر والتدبير، أو مقتضيات الشفافية اللاحقة. وبهذا تتحول المادة عمليًا إلى مدخل قابل للاستدعاء على طيف واسع من الحالات، من إدارة جزئية للشبكة إلى القطع الشامل.

ويتعزز هذا المعنى عندما تُقرأ المادة 67 داخل منظومة قانون الاتصالات نفسها. فالقانون يتعامل، في الأصل، مع استمرارية الخدمة بوصفها التزامًا على المرخص لهم، إذ تشير المادة 25[65] إلى أن الترخيص يحدد التزامات المرخص له، ومن بينها "الالتزام باستمرار تقديم الخدمة والإجراءات الواجبة الاتباع في حالة قطع الخدمة أو إيقافها".

---

[64] المادة 67: للسلطات المختصة في الدولة أن تخضع لإدارتها جميع خدمات وشبكات اتصالات أي مشغل أو مقدم خدمة وأن تستدعي العاملين لديه القائمين على تشغيل وصيانة تلك الخدمات والشبكات وذلك في حالة حدوث كارثة طبيعية أو بيئية أو في الحالات التي تعلن فيها التعبئة العامة طبقا لأحكام القانون رقم 87 لسنة 1960 المشار إليه وأية حالات أخرى تتعلق بالأمن القومي.

[65] المادة 25: يحدد الترخيص الصادر التزامات المرخص له والتي تشمل على الأخص ما يأتي:
1- نوع الخدمة والتقنية المستخدمة.
2- مدة الترخيص.
3- الحدود الجغرافية لتقديم الخدمة وخطة التغطية السلكية واللاسلكية ومراحل تنفيذها.
4- مقاييس جودة وكفاءة الخدمة.
5- الالتزام باستمرار تقديم الخدمة والإجراءات الواجبة الإتباع في حالة قطع الخدمة أو إيقافها.
6- تحديد سعر الخدمة وطرق التحصيل والالتزام بالإعلان عن ذلك.
7- إتاحة الخدمة لجمهور المستخدمين دون تمييز.
8- الالتزام بنظام الترقيم القومي الذي يضعه الجهاز.
9- مراعاة متطلبات الخدمة الشاملة.
10- تقديم خدمات اتصالات الإغاثة والطوارئ مجانا وتوفير خدمة الدليل، وذلك كله طبقا لنوع الخدمة المرخص بها.
11- الالتزامات الخاصة بعدم المساس بالأمن القومي.
12- الالتزامات الخاصة بالقواعد الفنية المتعلقة بالسلامة الصحية والبيئية والتخطيطية والإنشائية الواجبة الإتباع طبقا للمعايير التي يتم وضعها بالاتفاق مع الوزارات والجهات المعنية بالدولة.
13- الإسهام في مجال البحث العلمي والتدريب.
14- الالتزام بما يحدده الجهاز مقابل الأعباء التي يتحملها في سبيل التحقق من وفاء المرخص له بالتزاماته وكذلك التأمينات المالية وجميع المستحقات الدورية.
15- تقديم ما يطلبه الجهاز من المعلومات والبيانات المتصلة بموضوع الترخيص.
16- الوفاء بالجزاءات المالية والتعويضات.
17- تقديم الخدمات في ظل قواعد المنافسة الحرة.

وجود هذا النص يعكس منطقًا تنظيميًا يرى القطع حدثًا استثنائيًا يستوجب إجراءات. لكن المادة 67 تعمل كاستثناء حاكم يسمح بنقل الإدارة إلى الدولة في حالات واسعة، ما يجعل "استمرارية الخدمة" مشروطة بقرار سيادي/أمني عند تفعيل الاستثناء.

ويضع قانون تنظيم الاتصالات آلية واضحة لإلزام مقدمي الخدمة بالاستجابة لطلبات وقرارات جهات الأمن القومي، حيث تعاقب (المادة 82)[66] من القانون بالحبس كل من خالف أوامر الاستدعاء المنصوص عليها في المادة 67، مع تشديد العقوبة في زمن الحرب أو التعبئة العامة مع أحتمال صدور قرار من المحكمة بوقف الترخيص بشكل مؤقت لحين الاستجابة لطلب الأستدعاء.

المغزى هنا أن صلاحية الدولة لا تعمل فقط عبر طلب تعاون الشركات، بل عبر قابلية قانونية لفرض التنفيذ ومعاقبة الامتناع، وهو ما يضع مقدمي الخدمة في علاقة امتثال شبه قسرية عندما تُستدعى المادة 67.

ومن ناحية التطبيق، فتبرز واقعة 28 يناير 2011 بوصفها المثال الأكثر دلالة على قدرة الدولة على الانتقال من التحكم الجزئي إلى القطع الشامل. خطّ مسار الزمني للرقابة على الإنترنت يوثق أن الحدث الأبرز في 2011 كان قطع خدمات الإنترنت والاتصالات على مستوى الجمهورية يوم 28 يناير.[67]

إن أثر قطع الاتصالات لا ينحصر في حرية التعبير؛ إذ يعمل القطع كبنية تعطيل شاملة لقدرة المجتمع على التنظيم والتوثيق والوصول للمعلومات والخدمات الأساسية، لأن الإنترنت ليس وسيط نشر فقط بل شبكة تنسيق واعتماد يومي. وبالتالي فإن قانون الاتصالات يمنح الدولة، عبر المادة 67، قدرة واسعة على التحكم في الشبكة نفسها، ويعزز تنفيذها بنصوص تُجرّم الامتناع عن الاستجابة لأوامر الاستدعاء، يصبح القطع جزءًا من أدوات إدارة المجال العام الرقمي عبر التحكم في إمكانية الاتصال ذاتها، وليس فقط عبر التعامل مع المحتوى فقط.

18- وضع نظام لتلقي الشكاوى والتحقيق فيها وإصلاح الأعطال بكفاءة.
19- ضمان سرية الاتصالات والمكالمات الخاصة بعملاء المرخص له ووضع القواعد اللازمة للتأكد من ذلك.

[66] مادة 82: يعاقب بالحبس كل من خالف أوامر الاستدعاء المنصوص عليها فى المادة (67) من هذا القانون.
وتكون العقوبة السجن إذا وقعت الجريمة فى زمن الحرب أو فى الحالات التى تعلن فيها التعبئة العامة طبقًا لأحكام القانون رقم 87 لسنة 1960 فى شأن التعبئة العامة.

[67] عُزلة.. عن قطع الاتصالات أثناء ثورة يناير 2011، مؤسسة حرية الفكر والتعبير، مارس 2018، الرابط: https://afteegypt.org/research/monitoring-reports/2018/03/29/14918-afteegypt.html

ثاني عشر: تجريم التشفير وإخفاء الهوية



حماية الاتصال والخصوصية في المجال الرقمي

تُظهر التشريعات المصرية أن التشفير لا يُعامل بوصفه ضمانة وقائية ملازمة للخصوصية وسلامة الاتصالات، بل بوصفه قدرة تُدار بمنطق الإذن المسبق. هذا التموضع القانوني يعيد تعريف العلاقة بين المستخدم والتقنية، وبدلًا من أن يكون التشفير وسيلة افتراضية لحماية الاتصال من الاعتراض غير المشروع، يصبح استعماله مشروطًا بموافقات، بما يجعل الحماية قابلة للتعليق من حيث التصميم، لا فقط عند إساءة الاستخدام.

يتجسد ذلك بصورة مباشرة في قانون تنظيم الاتصالات رقم 10 لسنة 2003، حيث تُلزم (المادة 64)[68] مشغلي ومقدمي خدمات الاتصالات والتابعين لهم وكذلك مستخدمي هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من الجهاز والقوات المسلحة وأجهزة الأمن القومي، مع استثناء أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني. وإدراج المستخدمين ضمن المخاطبين بالحظر يجعل القاعدة لا تتعلق فقط بالبنية التحتية أو بالمشغلين، بل تمتد إلى المستوى الفردي، وهو ما ينقل التشفير من نطاق الحماية الشخصية إلى نطاق القدرة المقيدة إداريًا.

[68] المادة 64: يلتزم مشغلو ومقدمو خدمات الاتصالات والتابعون لهم وكذلك مستخدمو هذه الخدمات بعدم استخدام أية أجهزة لتشفير خدمات الاتصالات إلا بعد الحصول على موافقة من كل من الجهاز والقوات المسلحة وأجهزة الأمن القومي، ولا يسري ذلك على أجهزة التشفير الخاصة بالبث الإذاعي والتليفزيوني.
ومع مراعاة حرمة الحياة الخاصة للمواطنين التي يحميها القانون يلتزم كل مشغل أو مقدم خدمة أن يوفر على نفقته داخل شبكة الاتصالات المرخص له بها كافة الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات والتي تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصها في حدود القانون، على أن يتزامن تقديم الخدمة مع توفير الإمكانيات الفنية المطلوبة، كما يلتزم مقدمو ومشغلو خدمات الاتصالات ووكلائهم المنوط بهم تسويق تلك الخدمات بالحصول على معلومات وبيانات دقيقة عن مستخدميها من المواطنين ومن الجهات المختلفة بالدولة.

ويزداد أثر هذا التنظيم لأن مخالفة هذا المسار ليست مجرد مخالفة تنظيمية؛ فالمادة (81)[69] تقرر عقوبة الحبس والغرامة على من يخالف أحكام المادة (64)، وتضيف -فضلًا عن ذلك- أثرًا يمس التراخيص بوقفها مؤقتًا لحين توفير المعدات والنظم وبرامج الاتصالات المشار إليها.

وجود عقوبة سالبة للحرية هنا يجعل القاعدة ذات أثر ردعي مرتفع حتى دون إعلان موسع عن كيفية تطبيقها على التقنيات الحديثة، لأن مساحة "ما الذي يُعد جهاز تشفير" تبقى مرهونة بالتفسير، ما يُنتج عدم يقين يدفع إلى تجنب أدوات وقائية أو التردد في استخدامها، خصوصًا لدى الفئات الأكثر تعرضًا للمخاطر مثل الصحفيين والباحثين والنشطاء.

وفي الوقت نفسه، لا تعمل قيود التشفير منفصلة عن بقية المنظومة المصرية. فقانون مكافحة جرائم تقنية المعلومات -كما ذكرنا سابقًا- يفرض على مقدمي الخدمة الاحتفاظ بسجل وبيانات استخدام العملاء لمدة 180 يومًا، بما يشمل بيانات التعريف وبيانات حركة الاتصالات وغيرها من البيانات التي تمكّن من تتبع الأنماط. هذا يعني أن جزءًا كبيرًا من قابلية الرصد والتحليل لا يتوقف على فك محتوى الرسائل، لأن بنية الاحتفاظ نفسها تُبقي بيانات الحركة والربط الشبكي متاحة ضمن التزام قانوني قائم.

وتظهر مفارقة إضافية في اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات، التي تُلزم مقدمي خدمات تقنيات المعلومات باتخاذ إجراءات تقنية من بينها تشفير البيانات والمعلومات بما يحافظ على سريتها باستخدام معيار تشفير محدد (AES-128) مع تحميل مقدم الخدمة مسؤولية الحفاظ على سرية وأمان مفتاح التشفير.[70] وهذا يبيّن أن المنظومة القانونية تميل إلى نموذج تشفير مُدار تتحكم فيه جهة الخدمة وتحتفظ بمفاتيحه داخل ترتيبات الامتثال، في مقابل تضييق مساحة التشفير الذي يتحكم فيه المستخدم أو الذي يقع خارج منظومة الموافقات المسبقة.

وبهذا تتشكل سياسة مزدوجة تعتمد على مسار يضع استخدام التشفير في الاتصالات تحت منطق الإذن والعقاب، ومسار موازٍ يبني قدرة واسعة على التحليل عبر الاحتفاظ بالبيانات وتمكين الامتثال التقني لدى مقدمي الخدمة. بحيث يتحول التشفير من حق وقائي يعزز سرية الاتصال إلى أداة أمن معلومات داخل منظومة مُراقَبة، بينما تبقى حماية المستخدمين رهينة بإطار موافقات وممارسات قابلة للتوسع.

[69] المادة 81: يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه كل من خالف أيا من أحكام المادة (64) من هذا القانون. وتحكم المحكمة فضلا عن ذلك بوقف الترخيص مؤقتا لحين قيام المخالف بتوفير المعدات والنظم وبرامج الاتصالات المشار إليها في تلك المادة.

[70] المادة 2: يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2 و3) من الفقرة أولاً من المادة رقم (2) من القانون:
1 – تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسى متماثل أو غير متماثل لا يقل فى تأمينه عن (Advanced Encryption Standard (ASE-128 بمفتاح شفرة لا يقل عن (128 بت)، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير.
.....
3 – استخدام بروتوكولات آمنة، مثل بروتوكول نقل النص التشعبى المؤمنHTTPS
.....
11 – استخدام معدات وأجهزة ونظم وبرمجيات الجدران النارية (NGFW-UTM-Firewalls) لحماية الشبكات والنظم

ثالث عشر: تجريم حيازة التقنيات المتطورة... الدرونز نموذجًا

يعكس تنظيم الطائرات المسيّرة في مصر نمطًا تشريعيًا أوسع يقوم على التعامل مع القدرة التقنية بوصفها محل اشتباه سابق على الفعل، وليس بوصفها أداة يمكن تنظيم مخاطر استخدامها. فالقانون لا يبدأ بتحديد استخدامات ضارة بعينها ثم تجريمها، بل يضع حظرًا عامًا يشمل الاستيراد والتصنيع والتجميع والتداول والحيازة والاتجار والاستخدام، ثم يجعل الإباحة ممكنة فقط عبر تصريح صادر من جهة سيادية.

يبدأ تنظيم استحدام الدرونز في المادة الأولى تعريف شديد الاتساع في القانون رقم 216 لسنة 2017[71]؛ إذ لا يميز بين فئات تقنية أو درجات خطورة، بل يتبنى تعريفًا يضم أي جسم يمكنه الطيران بدون طيار أيا كان شكله أو حجمه ويمكن تحميله بأحمال إضافية مما يمثل تهديدًا للأمن القومي ويتم تشغيله أو التحكم فيه عن بعد. وإدراج عبارة "يمثل تهديدًا للأمن القومي" داخل التعريف نفسه يدمج الافتراض الأمني في بنية المفهوم القانوني، ويجعل نطاق الانطباق مفتوحًا بطبيعته، ويُصعّب على الأفراد توقع ما يقع تحت طائلة التجريم دون الرجوع إلى تقديرات لاحقة.

ثم يُعرّف القانون "الجهة المختصة" و"الوزير المختص" بوزارة الدفاع ووزير الدفاع. وذلك يعني الانتقال بآلية الترخيص من نموذج مدني (سلامة/ملاحة/ضوابط تشغيل) إلى نموذج سيادي تُدار فيه الإباحة عبر قرار مركزي يعلو على منطق السوق والتطبيقات المدنية والبحث العلمي والاستخدام الشخصي.

ويُترجم هذا التمركز إلى قاعدة حظر شاملة في المادة الثانية[72]، حيث يمتد المنع إلى الأشخاص الاعتبارية العامة والخاصة والأشخاص الطبيعيين، ولا يرفع الحظر إلا بتصريح"وفقًا للأحوال والشروط والإجراءات" التي تحددها اللائحة التنفيذية. وبالتالي فإن الحيازة نفسها تُعامل كواقعة مجرّمة في حال غياب التصريح، بما ينقل القانون من تجريم الاستخدام الضار إلى تجريم سابق على الاستخدام.

[71] المادة الأولى قانون رقم 216 لسنة 2017 بتنظيم استخدام الطائرات المحركة آليًا أو لاسلكيًا
"في تطبيق أحكام هذا القانون، يُقصد بالعبارات التالية المعنى المبين قرين كل منها:
1 – الطائرات المحركة آليًا أو لاسلكيًا: أى جسم يمكنه الطيران بدون طيار دون اتصال الغير به باستخدام أى من أنواع التقنيات، وأيًا كان شكله أو حجمه، ويمكن تحميله بأحمال إضافية، سواء كانت أجهزة أو معدات أو أنظمة تسليح أو ذخائر أو مفرقعات أو غيرها مما يمثل تهديدًا للأمن القومى للبلاد، ويتم تشغيله أو التحكم فيه عن بعد.
2 – الجهة المختصة: وزارة الدفاع.
3 – الوزير المختص: وزير الدفاع."

[72] المادة الثانية قانون رقم 216 لسنة 2017 بتنظيم استخدام الطائرات المحركة آليًا أو لاسلكيًا
"يُحظر على وحدات الجهاز الإدارى للدولة من وزارات ومصالح وأجهزة ووحدات الإدارة المحلية والهيئات العامة والشركات وغيرها من الأشخاص الاعتبارية العامة أو الخاصة والأشخاص الطبيعيين، استيراد أو تصنيع أو تجميع أو تداول أو حيازة أو الاتجار أو استخدام الطائرات المحركة آليًا أو لاسلكيًا، إلا بعد الحصول على تصريح بذلك من الجهة المختصة، وذلك وفقًا للأحوال والشروط والإجراءات التى تحددها اللائحة التنفيذية لهذا القانون مع مراعاة أحكام قانون الطيران المدنى الصادر بالقانون رقم 28 لسنة 1981"



شكل (13): نظام التصاريح والعقوبات في قانون الطائرات المسيّرة

وتكشف اللائحة التنفيذية (قرار رئيس مجلس الوزراء رقم 931 لسنة 2018) أن التصريح إطار ضبط تفصيلي يُعرَّف بأنه المستند الصادر لمزاولة الاستيراد أو التصنيع أو التجميع أو التداول أو الحيازة أو الاتجار أو الاستخدام للطائرات المسيّرة[73]، وتحدد أن طلب التصريح يقدم إلى هيئة عمليات القوات المسلحة. كما تضع قاعدة إجرائية دالة وهي البت خلال 30 يومًا، واعتبار انقضاء المدة دون رد هي بمثابة رفض، مع صلاحية إصدار التصريح لمدة لا تجاوز 3 سنوات وتسجيله في سجل مخصص.

وتضيف اللائحة طبقة امتثال مستمرة عبر إلزام المصرح له بإمساك سجلين (أحدهما للطائرات ومواصفاتها وجهة الحصول عليها، والآخر لتواريخ التداول والاستخدام)، مع خضوعهما لمراجعة مختصين تحددهم الجهة المختصة، وإجراءات خاصة في حال انتهاء النشاط أو عدم تجديد التصريح، بما في ذلك عدم التصرف في الطائرات وإبلاغ الجهة المختصة خلال ثلاثة أيام لحين "تقنين

[73] مادة 2 من قرار رئيس مجلس الوزراء رقم 931 لسنة 2018 بإصدار اللائحة التنفيذية للقانون رقم 216 لسنة 2017
يتم استيراد وتصنيع وتجميع وتداول وحيازة والاتجار واستخدام الطائرات المحركة آليًا أو لاسلكيًا وفقًا للقواعد والإجراءات الآتية:

1" – يقدم طلب الحصول على التصريح إلى هيئة عمليات القوات المسلحة مستوفيًا المستندات التى يصدر بتحديدها قرار من الوزير المختص.

2 – يدرج بالطلب عدد الطائرات المطلوب التصريح بها ومواصفاتها وجهة الحصول عليها.

3 – يتم البت فى الطلب بالقبول أو الرفض خلال ثلاثين يومًا من تاريخ تقديمه، ويعتبر مضى المدة دون رد بمثابة رفض.

4 – تصدر الجهة المختصة التصريح لمدة لا تجاوز ثلاث سنوات، وتخطر المصرح له بخطاب مسجل بعلم الوصول، مع موافاة الجهة ذات الاختصاص بصورة منه.

5 – يجدد التصريح بطلب من المصرح له على الجهة المختصة قبل ثلاثة أشهر من تاريخ انتهائه.

6 – يخصص بالجهة المختصة سجل تقيد فيه التصاريح الصادرة وتاريخها والمصرح لهم.

7 – يلتزم المصرح له بإمساك سجلين أحدهما لتسجيل ما لديه من طائرات ومواصفات وجهة الحصول عليها، والآخر يقيد فيه تاريخ تداول واستخدام الطائرات، وتسرى عليهما أحكام القيد فى السجلات التجارية، ويتولى المراجعة عدد من المختصين الذين تحددهم الجهة المختصة.

8 – فى حال عدم الموافقة على تجديد التصريح أو انتهاء النشاط المصرح به، يلتزم المصرح له بعدم التصرف فيما لديه من طائرات وإبلاغ الجهة المختصة، فيما لا يجاوز ثلاثة أيام، بكافة بيانات هذه الطائرات، وذلك لحين تقنين موقفها أو صدور قرار فى هذا الشأن."

الموقف" أو صدور قرار. كما تقرر مسار تظلم أمام لجنة يُصدر بتشكيلها وبيان إجراءاتها قرار من وزير الدفاع، بما يجعل المراجعة داخل الإطار نفسه الذي أصدر القرار.

ولا تكتفي اللائحة بإجراءات عامة، بل تُجزّئ التصاريح بحسب الغرض (اقتصادي/تجاري، رياضي، علمي/بحثي)، وتضيف شروطًا تتجاوز الجوانب الفنية إلى منظومة موافقات أمنية ومدنية: إذ تتطلب—في الأنشطة الاقتصادية والرياضية والبحثية—موافقات أمنية من جهات محددة، وموافقة وزارة الطيران المدني وجهات الدولة المختصة، مع تحديد الغرض والنطاق المكاني والزماني للاستخدام. وفي المجال البحثي تفرض إقرارًا بعدم الاستخدام إلا في حدود الغرض العلمي، مع استثناء محدود لجامعات ومعاهد يتضمن هيكلها الأكاديمي قسمًا للطيران وبشروط مكانية مرتبطة بنطاق المؤسسة.

وتكشف قراءة اللائحة كذلك أن الاستثناء لا يعمل تلقائيًا حتى في الحالات "الأخف". فمقال مسار التحليلي يبين أن اللائحة أشارت إلى إعفاء بعض الأنواع ذات مواصفات تقنية شديدة التقييد (مثل الوزن الخفيف جدًا وغياب GPS أو الطيران الآلي وقيود المسافة والارتفاع وعدم قابلية حمل أي حمولة)، لكنها مع ذلك تربط التحقق من الإعفاء بمسار فحص يتضمن تقريرًا من مصلحة الجمارك ومراجعة مختصين بوزارة الدفاع خلال 30 يومًا. بهذا تتحول حتى "استثناءات الألعاب" إلى منطقة امتثال إجرائي، لا إلى مساحة واضحة يُمكن للمستخدم العادي الركون إليها دون مخاطرة.

أما العقوبات، فتؤكد أن المقصود ليس "تنظيم استخدام" بقدر ما هو "تجريم شامل" لغياب التصريح. فالمادة الثالثة تقرر الحبس من سنة إلى سبع سنوات وغرامة، مع تشديد يصل إلى السجن المؤبد إذا كان الفعل لغرض إرهابي، وإلى الإعدام إذا ترتبت وفاة. وتضيف المصادرة في جميع الأحوال لصالح القوات المسلحة، بما يجعل الأثر العقابي مركبًا: حرمان من الحرية وحرمان من الملكية.

ويكتسب الإطار بعدًا إضافيًا عبر المادة الرابعة التي تمنح أعضاء الضبط القضائي العسكري صفة مأموري الضبط القضائي فيما يتعلق بتطبيق القانون ولائحته والقرارات الصادرة تنفيذًا له. هذا يرسّخ أن مسار الإنفاذ ليس مدنيًا خالصًا، بل يعتمد على أدوات ضبط ذات طبيعة عسكرية في المتابعة والتفتيش والتحقق من الامتثال للسجلات وشروط التصريح.

في المحصلة، يقدم تنظيم الدرونز نموذجًا متكاملًا لـ"تجريم التكنولوجيا": تعريف واسع يُدرج الافتراض الأمني في صلب المفهوم، حظر شامل للأفعال بما فيها الحيازة، ترخيص سيادي عبر وزارة الدفاع وإجراءات امتثال مستمرة، عقوبات سالبة للحرية ومصادرة إلزامية، ومسار إنفاذ يتضمن الضبط القضائي العسكري. ويزداد وزن هذا النموذج بالنظر إلى اتساع الاستخدامات المدنية الممكنة للطائرات المسيّرة (في الزراعة، ورصد البنية التحتية، والاستجابة الإنسانية، وتوصيل الإمدادات)، ما يجعل الحظر العام مع استثناء بالتصريح لا ينظم "المخاطر" فقط، بل يحدد عمليًا حدود تطور الاستخدامات المدنية ذاتها وفق منطق أمني سابق على السوق والابتكار.

يعكس تنظيم الطائرات المسيّرة في مصر نمطًا تشريعيا أوسع يقوم على تحويل التقنيات المتقدمة من أدوات يمكن تنظيم مخاطرها إلى "موضوع جنائي" تُجرَّم حيازته في ذاته. هذا الاختيار لا يستهدف سلوكًا ضارًا محددًا، بل يوسّع دائرة الاشتباه لتشمل الملكية والحيازة والتداول والاستخدام، ثم يربط رفع التجريم بتصريح تصدره جهة سيادية خارج المجال المدني. يترتب على ذلك تجريم واسع يسبق الفعل، ويحوّل التكنولوجيا إلى قرينة خطر، ويمنح الدولة سلطة عقابية واستبعادية.

الإطار الأوضح هو القانون رقم 216 لسنة 2017 بشأن تنظيم استخدام الطائرات المحركة آليًا أو لاسلكيًا وتداولها والاتجار فيها. القانون يعرّف هذه الطائرات تعريفًا شديد الاتساع: "أي جسم يمكنه الطيران بدون طيار... باستخدام أي من أنواع التقنيات... وأيًا كان شكله أو حجمه... ويمكن تحميله بأحمال إضافية... مما يمثل تهديدًا للأمن القومي... ويتم تشغيله أو التحكم فيه عن بعد". هذا التعريف لا يقتصر على فئة تقنية محددة ولا يضع معيارًا فنيًا قابلًا للتحقق، بل يدمج الوصف التقني بادعاء أمني "يمثل تهديدًا

للأمن القومي" داخل التعريف نفسه، بما يجعل مجال الانطباق مفتوحًا بطبيعته، ويصعّب على الأفراد توقع ما يقع تحت طائلة التجريم.

الأهم أن القانون يحسم أن "الجهة المختصة" هي وزارة الدفاع، وأن "الوزير المختص" هو وزير الدفاع. هذه ليست تفصيلة إدارية؛ هي قرار تموضع قانوني يجعل الترخيص مسألة سيادية لا تنظيمًا مدنيًا للسلامة أو الخصوصية أو المجال الجوي. وفي المادة التالية يوسّع القانون نطاق الحظر على نحو صريح ليشمل الحيازة والتداول والاتجار والاستيراد وغير ذلك، ويقصر الإباحة على الحصول على "تصريح" من الجهة المختصة ووفق شروطها وإجراءاتها. بهذا تتحول الحيازة العادية لتقنية إلى واقعة مُجرّمة ما لم تُرفق بإذن مسبق، بدل أن يكون التجريم مرتبطًا بالاستخدام الضار أو الانتهاكي.

العقوبات تؤكد أن المسألة ليست "ترخيصًا تنظيميًا" بل تجريمًا جنائيًا كاملًا. ينص القانون على الحبس مدة لا تقل عن سنة ولا تجاوز سبع سنوات، وغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى العقوبتين، لكل من استورد أو صنع أو جمع أو تداول أو حاز أو أحرز أو استخدم هذه الطائرات بالمخالفة لنظام التصريح. ثم يقرر تشديدًا نوعيًا يصل إلى السجن المؤبد إذا ارتكبت الأفعال "لغرض إرهابي"، ويصل إلى الإعدام إذا ترتب على الفعل وفاة شخص. ويضيف الحكم بالمصادرة كقاعدة، بما يجعل الأثر العقابي مزدوجًا حرمان من الحرية وحرمان من الملكية. والأكثر دلالة هو إسناد الاختصاص بالقضايا المتعلقة بتطبيق القانون ولائحته إلى القضاء العسكري فيما يتصل بالتطبيق والضبط القضائي. هذا يرسّخ نقل نزاع تقني-مدني إلى نطاق محاكمة استثنائي بطبيعته، ويضغط على ضمانات المحاكمة العادلة ويضعف الرقابة القضائية المدنية الفعّالة.

لذلك فإن تنظيم الدرونز في مصر يقدم نموذجًا مكتملًا لتجريم التقنيات المتطورة تعريف واسع، حظر شامل يشمل الحيازة، ترخيص سيادي غير مدني، عقوبات سالبة للحرية مشددة، واختصاص قضائي عسكري. هذا النموذج قابل للتمدد إلى تقنيات أخرى كلما أرادت الدولة تحويل "القدرة التقنية" إلى "شبهة قانونية" بدلاً من تنظيم الاستخدامات الضارة بضمانات واضحة.

التوصيات



1. إصلاح تشريعي يعيد تعريف الاستثناء ويضيّق المعايير

ينبغي مراجعة وتعديل النصوص التي تُجيز الحجب أو الوقف أو التعطيل أو تقييد المحتوى بحيث تُربط بمعايير محددة لا فضفاضة، مع تعريفات منضبطة لعبارات مثل الأمن القومي والخطر الوشيك والقيم الأسرية، حتى لا تتحول إلى بوابات مفتوحة لتوسيع القيد.

ويلزم إعادة ترتيب العلاقة بين القانون والقرار الإداري، بحيث لا يُنتج القرار الإداري أثرًا جسيمًا على الحقوق دون أساس قانوني واضح ومحدد، ودون رقابة قضائية سريعة وفعّالة.

2. ضمانات إجرائية واضحة في الحجب وتقييد المحتوى

يجب أن يُبنى أي إجراء يمس النفاذ إلى المواقع أو الحسابات على مبدأ الإخطار والبيان المكتوب للأسباب، وعلى حق الطعن الفوري أمام قاضٍ مستقل خلال مدد قصيرة. ويستحسن تبني قاعدة أن الأصل هو وقف الإجراء عند الطعن إذا ترتب عليه ضرر جسيم يصعب تداركه، مع إلزام الجهات المختصة بنشر بيانات دورية مجمعة عن عدد أوامر الحجب ونطاقها وأساسها القانوني، بما لا يضر بتحقيقات محددة.

3. إنهاء تحويل الترخيص إلى شرط وجود للمواقع الرقمية

ينبغي فصل تنظيم العمل الإعلامي المهني عن فكرة إذن الوجود الرقمي. بحيث يتم الاعتماد على نظام إخطار بسيط للمواقع الصحفية المستقلة بدل الترخيص المُسبق المكلف، مع رسوم متناسبة مع طبيعة النشر الرقمي، ومع قاعدة تمنع تعطيل الطلبات بالسكوت وتعتبر عدم الرد خلال مدة محددة موافقة، أو على الأقل تُلزم الجهة الإدارية بقرار مُسبب قابل للطعن السريع.

كما يلزم تقليص الاشتراطات التشغيلية التي تُحوّل التنظيم إلى سيطرة ممتدة، ووضع ضمانات دقيقة لأي التزام بأرشفة المحتوى أو توطين الخوادم، بما يحمي أمن البيانات ويمنع التعسف.

4. حماية الخصوصية عبر تقليص الاحتفاظ الإلزامي بالبيانات وضبط النفاذ

يجب مراجعة قواعد الاحتفاظ الإلزامي بالبيانات لتقليل المدد والنطاق، وربط أي نفاذ إلى البيانات بمعيار الضرورة والتناسب وبأمر قضائي مسبب، مع توثيق الطلبات وإمكانية مراجعتها لاحقًا من جهة مستقلة.

كما ينبغي اعتماد قواعد أمن معلومات صارمة على الجهات الحائزة للبيانات، لأن مخاطر التسريب وسوء الاستخدام هي جزء من جوهر الحق في الخصوصية.

5. تقوية نظام حماية البيانات الشخصية واستقلال جهة الإنفاذ

يلزم تضييق الاستثناءات الواسعة التي تجعل الحماية قابلة للتعليق بسهولة، ووضع ضوابط موضوعية لطلبات الجهات الأمنية بحيث لا تتحول إلى أوامر إدارية ملزمة بلا رقابة.

كما ينبغي تعزيز استقلال الجهة المنوط بها الإنفاذ وعلنية معاييرها وقراراتها، وتبسيط مسارات الشكوى للأفراد، وضمان حقهم في الاطلاع والتصحيح والمسح والاعتراض بآليات عملية وسريعة.

6. تقليل الاعتماد على التجريم الجنائي في ضبط التعبير الرقمي

ينبغي إعادة النظر في جرائم الأخبار الكاذبة بصيغها الفضفاضة التي تربط التجريم بأثر عام قابل للتأويل، ووضع معايير أدق تحمي النقاش العام والتحقق الصحفي.

كما ينبغي تقليص استخدام الحبس في قضايا النشر والتعبير، وتطوير بدائل مدنية متوازنة في السب والقذف تراعي الحق في السمعة دون تحويل المجال العام إلى ساحة تهديد جنائي دائم.

7. حماية التشفير وإخفاء الهوية بوصفهما أدوات أمان لا شبهة

ينبغي التعامل مع التشفير باعتباره وسيلة مشروعة لحماية الاتصال والخصوصية والعمل الصحفي والحقوقي، لا باعتباره قدرة مشروطة بإذن مسبق يطال المستخدمين.

وينبغي الإبقاء على تجريم الأفعال الضارة المحددة، لا تجريم الأدوات الوقائية في ذاتها، مع تبني سياسة واضحة تشجع أمن الاتصالات بدل دفع المستخدمين إلى الضعف التقني والخطر.

8. تنظيم التقنيات مزدوجة الاستخدام بمنطق المخاطر لا بمنطق الحظر الشامل

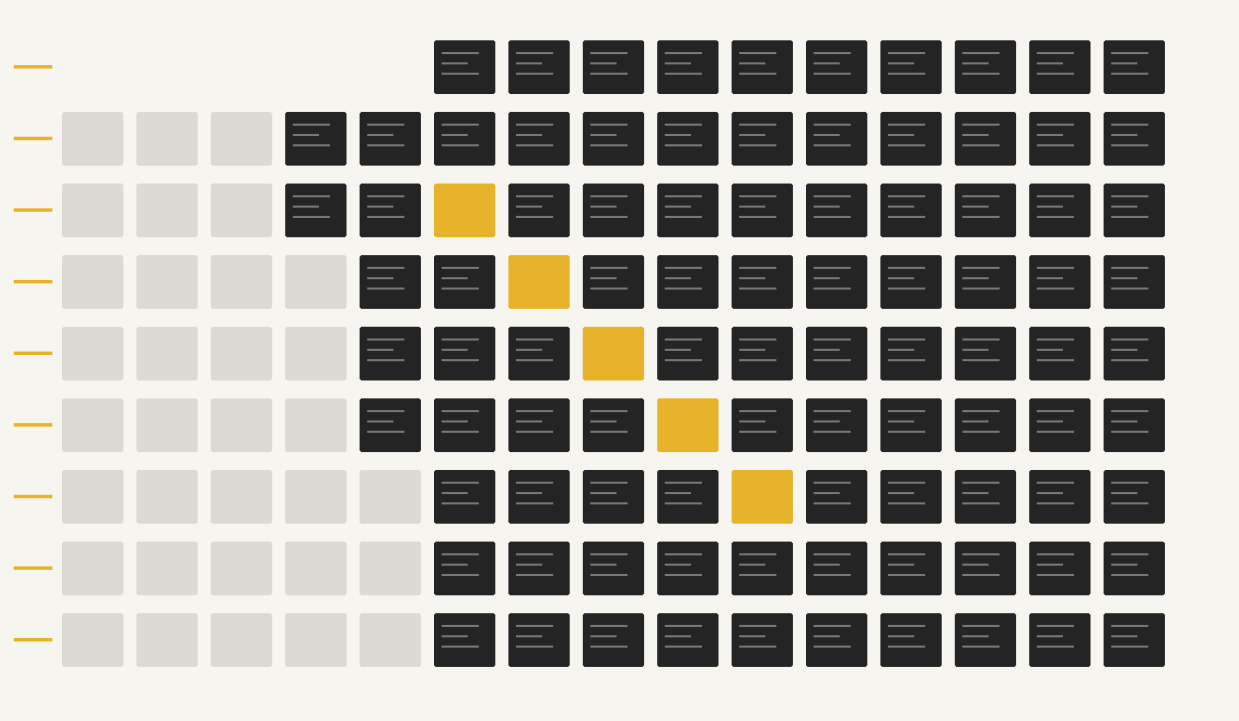
في موضوع معدات الاتصالات والدرونز وغيرها من التقنيات، يلزم الانتقال من منع شامل مع استثناء بالتصريح إلى تنظيم يميّز بين درجات الخطورة والاستخدامات المدنية والبحثية. ويشمل ذلك نشر قوائم ومعايير واضحة وسهلة الوصول، ووضع استثناءات عملية للصيانة والبحث والتجريب، وتدرج الجزاءات بحيث تكون العقوبة الجنائية آخر ملاذ، مع ضمان حق طعن فعّال على قرارات التصنيف أو الرفض.

9. ضمانات الحقوق الرقمية في قانون الإجراءات الجنائية قبل بدء نفاذه

مع إرجاء بدء العمل بقانون الإجراءات الجنائية الجديد إلى أكتوبر 2027، من الضروري وضع ضوابط تنفيذية تحمي من توسع المراقبة الرقمية وتتبع الأفراد تحت عنوان بدائل الحبس، وأن تُبنى هذه التدابير على الحد الأدنى الضروري وبمدة محددة وبإشراف قضائي فعلي.

كما يجب أن تتضمن ترتيبات التحقيق والمحاكمة عن بُعد ضمانات واضحة للسرية والعلانية وحق الدفاع وسلامة التسجيل والاحتفاظ، حتى لا تتحول الإجراءات الرقمية إلى طبقة مراقبة إضافية أو إلى اختلال دائم في توازن الخصومة.

الخاتمة



تكشف القراءة الحقوقية للفضاء الرقمي في مصر أن المشكلة لا تكمن في غياب النصوص بقدر ما تكمن في غياب حدود تشغيلية واضحة تمنع تحوّل التدخل الاستثنائي إلى ممارسة يومية. فعندما تتسع المعايير وتكبر مساحة السلطة التقديرية، تتراجع قابلية التوقع، ويزداد الامتثال الوقائي، وتظهر الرقابة الذاتية بوصفها النتيجة الأكثر شيوعًا؛ عندها يصبح الحق أقل حضورًا في الواقع حتى لو ظل مكتوبًا في النصوص.

وهذا الأثر لا يطال الأفراد وحدهم، بل يطال المجال العام كله، لأن الغموض القانوني يضعف الثقة ويقلل من قدرة المجتمع على النقاش والتحقق والمحاسبة، ويجعل تكلفة المشاركة أعلى من أن يتحملها كثيرون.

واستعادة الحقوق تتحقق بإعادة ضبط المنطق الحاكم للتنظيم، والإقرار بأن الأصل هو الإتاحة وحرية التعبير والاتصال، وأن أي تقييد يجب أن يستند إلى قانون واضح، وأن يكون ضروريًا ومتناسبًا وأقل الوسائل تقييدًا، وأن يخضع لرقابة مستقلة فعّالة ومسارات طعن سريعة ومفهومة، وأن يُحاط بحد أدنى من الشفافية يسمح بالمراجعة العامة ويقلل مخاطر التعسف. وهذه المطالب هي معايير مستقرة في الإطار الدولي لحرية التعبير والخصوصية في العصر الرقمي، حيث تُعد القيود المشروعة استثناءً مضبوطًا لا قاعدة مفتوحة.

ومتى اعتُبر الإنترنت وخدمات الاتصالات جزءًا من شروط ممارسة الحقوق والحياة اليومية والاقتصاد، تصبح حماية المجال الرقمي مسألة سيادة قانون بقدر ما هي مسألة أمن. وعندها لا يُقاس حضور الدولة باتساع قدرتها على التدخل، بل بقدرتها على إدارة المخاطر دون تآكل الثقة العامة، ودون تحويل المجتمع إلى دائرة اشتباه دائمة، ودون إضعاف الحقوق التي يفترض أن التنظيم وُجد لحمايتها.