



بتمويل من  
الاتحاد الأوروبي



مكتب الأمم المتحدة  
لمكافحة الإرهاب  
مركز الأمم المتحدة لمكافحة الإرهاب



## أمن الفضاء الإلكتروني والتكنولوجيات الجديدة



إنشاء الإطار التشريعي،  
وآليات الشفافية  
والرقابة لجمع البيانات  
عبر الإنترنت



## إخلاء مسؤولية

لا تعكس الآراء والاستنتاجات والنتائج والتوصيات المُعبّر عنها في هذه الوثيقة بالضرورة آراء منظمة الأمم المتحدة أو المنظمة الدولية للشرطة الجنائية (الإنتربول) أو حكومات الاتحاد الأوروبي أو أيًا من الكيانات الوطنية أو الإقليمية أو الدولية المشاركة فيها. لا تنطوي التسميات المستخدمة في هذا المنشور ولا المواد المعروضة فيه على الإعراب عن أي رأي كان من جانب الأمانة العامة للأمم المتحدة إزاء الوضع القانوني لأي بلد أو إقليم أو مدينة أو منطقة أو للسلطات القائمة فيها أو إزاء تعيين حدودها أو تخومها. يسمح باقتباس محتويات هذا المنشور أو إعادة إنتاجها شريطة الاعتراف بمصدر المعلومات. كما يود المؤلفون الحصول على نسخة من الوثيقة التي استخدمت هذا المنشور أو اقتبست عنه.

## شكر وتقدير

هذا التقرير نتاج مبادرة مشتركة بين مركز الأمم المتحدة لمكافحة الإرهاب التابع لمكتب الأمم المتحدة لمكافحة الإرهاب والإنتربول من أجل تعزيز قدرات سلطات إنفاذ القانون وسلطات العدالة الجنائية على مكافحة استخدام التكنولوجيات الجديدة لأغراض الإرهاب. وقد مُولت هذه المبادرة المشتركة بمساهمات سخية من الاتحاد الأوروبي.

## حقوق النشر

© مكتب الأمم المتحدة لمكافحة الإرهاب، 2023.

مكتب الأمم المتحدة لمكافحة الإرهاب، مقر الأمم المتحدة،

نيويورك، نيويورك 10017.

[www.un.org/counterterrorism](http://www.un.org/counterterrorism)

© المنظمة الدولية للشرطة الجنائية (الإنتربول)، 2023.

200، رصيف شارل ديغول 69006 ليون، فرنسا.

[www.interpol.int/en](http://www.interpol.int/en)

# المحتويات

4	توطئة مشتركة	4
5	شكر وتقدير	5
5	مصطلحات وتعريف	5
7	ملخص تنفيذي	7
	<b>[أولاً]</b>	
8	خلفية	8
8	لمحة عامة	1 - 1
9	مبادرة التكنولوجيا لمكافحة الإرهاب	2 - 1
10	أغراض الوثيقة واستخداماتها	3 - 1
	<b>[ثانياً]</b>	
12	النهج	12
12	لمحة عامة	1 - 2
12	الإطار التوجيهي	2 - 2
14	المنهجية	3 - 2
	<b>[ثالثاً]</b>	
16	مقدمة	16
16	لمحة عامة	1 - 3
16	التكنولوجيات الجديدة ومكافحة الإرهاب	2 - 3
	<b>[رابعاً]</b>	
20	جمع البيانات عبر الإنترنت من قبل سلطات إنفاذ القانون	20
20	لمحة عامة	1 - 4
21	المصطلحات: جمع البيانات والمراقبة عبر الإنترنت	2 - 4
22	البيانات الوصفية	3 - 4
22	المبادئ التوجيهية	4 - 4
24	حقوق أصحاب البيانات	5 - 4
	<b>[خامساً]</b>	
26	الشفافية وآليات الرقابة	26
26	لمحة عامة	1 - 5
26	هيئات الرقابة الفعالة	2 - 5
27	الموافقة المستقلة المسبقة لعمليات المراقبة والتحقيق الخاصة	3 - 5
29	آليات الشكاوى	4 - 5
31	البيانات المجمعة تجارياً	5 - 5
	<b>[سادساً]</b>	
32	ملخص الاعتبارات	32
32	الاعتبارات الرئيسية	1 - 6

## توطئة مشتركة

جذب التقدم المحرز في مجال تكنولوجيا المعلومات والاتصالات كلاً من الجماعات الإرهابية والجماعات المتطرفة العنيفة لاستغلال هذا التقدم في تسهيل قيامهم بمجموعة واسعة من الأنشطة التي تشمل التحريض ونشر التشدد والتجنيد والتدريب والتخطيط وجمع المعلومات والتواصل والتحضير والدعاية والتمويل. ويستمر الإرهابيون في استكشاف آفاق تكنولوجية جديدة، في حين أن الدول الأعضاء ما زالت تعرب عن قلقها المتزايد حيال استخدام التكنولوجيات الجديدة لأغراض إرهابية.

طلبت الدول الأعضاء خلال الاستعراض السابع لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب مكتب الأمم المتحدة لمكافحة الإرهاب والكيانات الأخرى المنضوية في ميثاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب "بتقديم دعم مشترك للإجراءات والنهج المبتكرة لبناء قدرات الدول الأعضاء، متى طلبت، على التعامل مع التحديات التي تنجم عن التكنولوجيات الجديدة واستغلال الفرص التي تقدمها في الوقاية والحد من الإرهاب ومكافحته، بما في ذلك الجوانب المرتبطة بحقوق الإنسان."

وفي تقريره المقدم للأمانة العامة عن أنشطة منظومة الأمم المتحدة في تطبيق استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/77/718)، يشدد الأمين العام على أن "[...] التكنولوجيات الجديدة والناشئة توفر فرصاً غير مسبوقه لتحسين رفاه البشرية بالإضافة إلى أدوات جديدة لمكافحة الإرهاب. [...] وعلى الرغم من تعزيز الجهود وتضافرها، إلا أن استجابة المجتمع الدولي غالباً ما تكون متأخرة. وبعض هذه الاستجابات تحدّ من حقوق الإنسان على نحو غير مبرر، ويشمل ذلك على وجه التحديد كلاً من الحق في الخصوصية وحق حرية التعبير، بما في ذلك الحق في التماس المعلومات وتلقيها."

ونسعى من خلال التقارير السبعة المشمولة في هذه الخلاصة - وهي نتاج الشراكة بين مركز الأمم المتحدة لمكافحة الإرهاب والمنظمة الدولية للشرطة الجنائية المندرجة تحت مبادرة التكنولوجيا لمكافحة الإرهاب (CT TECH) المشتركة والممولة من الاتحاد الأوروبي إلى دعم سلطات إنفاذ القانون والعدالة الجنائية التابعة للدول الأعضاء في مكافحة استغلال التكنولوجيات الجديدة والناشئة لأغراض الإرهاب وفي الاستفادة من التكنولوجيات الجديدة والناشئة لمحاربة الإرهاب كجزء من هذه الجهود، مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

إن مكتبنا على استعداد لمواصلة دعم الدول الأعضاء وغيرها من الشركاء في الوقاية والحد من الإرهاب ومكافحته بكافة أشكاله ومظاهره، والاستفادة من الآثار الإيجابية للتكنولوجيا في مكافحة الإرهاب.

ستيفن كافانا

المدير التنفيذي  
للخدمات الشرطة في الإنترنت



فلاديمير فورونكوف

وكيل الأمين العام، مدير مكتب الأمم المتحدة  
لمكافحة الإرهاب،  
المدير التنفيذي لمركز الأمم المتحدة لمكافحة الإرهاب



# شكر وتقدير

تم تطوير هذه الوثيقة بمساهمة مجموعة واسعة من أصحاب المصلحة كما تمت مراجعتها من قبلهم. يود مكتب الأمم المتحدة لمكافحة الإرهاب أن يعرب عن امتنانه للمساهمة التي قدمها:

- السيد كامل الهلالي – دكتوراه في القانون، جامعة بانثيون أساس، باريس

## مصطلحات وتعريف

<b>الذكاء الاصطناعي</b>	يستخدم عموماً لوصف التخصص المعني بتطوير الأدوات التكنولوجية التي تمارس أعمالاً بشرية، كالخطيط والتعلم والتفكير والتحليل.
<b>إجراءات العدالة الجنائية</b>	هي إجراءات قانونية لتوجيه تهم جنائية لفرد أو كيان وإجراءات المحكمة والحكم في القضية والعقوبة عند الإدانة وكذلك الإصلاح وإعادة التأهيل.
<b>الشبكة المظلمة</b>	الجزء المشفر من الإنترنت الذي يمكن الوصول إليه باستخدام برامج معينة لا تعتبر جريمة بحد ذاتها، مثل متصفح Tor. ومع ذلك، من المعلوم بأن الشبكة المظلمة تحتوي على العديد من المواقع والخدمات الإجرامية التي تستضيفها هذه الشبكات <sup>1</sup> .
<b>آليات الرقابة الفاعلة</b>	هي آليات مستقلة، مجهزة بالخبرات والكفاءات والمصادر المناسبة والكافية، تمتلك حرية الوصول الكامل وغير المقيد إلى المعلومات والمواقع والمسؤولين، ولديها تفويضات وسلطات محددة بموجب القانون لفحص الامتثال للقوانين المعنية، بما في ذلك حقوق الإنسان، وبدء التحقيقات والتحقيق الكافي في سلوكيات المسؤولين.
<b>الأدلة</b>	مصطلح رسمي للمعلومات التي تشكل جزءاً من المحاكمة، بمعنى أنها تستخدم لإثبات الجريمة المزعومة أو نفيها. تعتبر كافة الأدلة معلومات بينما لا تشكل جميع المعلومات أدلة. وبذلك تعتبر المعلومات الشكل الأولي والأصلي للأدلة <sup>2</sup> .
<b>آليات الرقابة المحايدة</b>	هي الآليات التي تبني القرارات على الحقائق ووفقاً للقانون، من دون أية قيود، أو تأثيرات أو حوافز أو ضغوط أو تهديدات أو تدخلات غير لائقة، مباشرة أو غير مباشرة، من أي جهة كانت أو لأي سبب كان <sup>3</sup> .

1 المركز الأوروبي للجرائم الإلكترونية، تقييم تهديدات الجريمة المنظمة عبر الإنترنت لعام 2019 (يوربول، 2019)، [https://www.europol.europa.eu/cms/sites/default/files/documents/iocta\\_2019.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf)

2 دليل المديرية التنفيذية للجنة مكافحة الإرهاب لتسهيل استخدام المعلومات التي تم جمعها ومعالجتها وحفظها ومشاركتها من قبل القوات المسلحة وقبولها كأدلة في المحاكم الجنائية الوطنية بغرض الملاحقة القضائية للجرائم الإرهابية (2019). [https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/cted\\_military\\_evidence\\_guidelines.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org/securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf)

3 مفوضية الأمم المتحدة السامية لحقوق الإنسان، المبادئ الأساسية بشأن استقلال القضاء، <https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-independence-judiciary>

<p>هي مستقلة عن الأهداف السياسية والاقتصادية والعسكرية أو غيرها. تتمتع بـ: 1) استقلال رسمي (بحكم القانون) يتطلب بقاءها خارج السلسلة البيروقراطية والهرمية ضمن وزارة ما أو وكالات حكومية أخرى؛ و2) استقلال فعلي (بحكم الواقع)، يتعلق بحق الوكالة في تقرير المصير حول استخدام الإجراءات المناسبة<sup>4</sup>.</p>	<p><b>آليات الإشراف المستقلة</b></p>
<p>هي ناتج جمع المعلومات ومعالجتها ونشرها وتحليلها وتفسيرها والتي جمعت من مصادر متعددة، بهدف إفادة صناعات القرار لأغراض التخطيط لاتخاذ القرارات أو الإجراءات - على المستوى الاستراتيجي أو التشغيلي أو التكتيكي. يجب جمع الاستخبارات وحفظها واستخدامها ومشاركتها وفقاً للالتزامات الدول الأعضاء المعنية بموجب القانون الدولي لحقوق الإنسان.</p>	<p><b>الاستخبارات</b></p>
<p>هي عملية جمع المعلومات (أو الأدلة) لتقرير ارتكاب الجريمة من عدمه، وتحديد الجاني وتقديم الأدلة التي تدعم الادعاء في الإجراءات القانونية.</p>	<p><b>التحقيقات الجنائية</b></p>
<p>تصف عادة إجراءات إنفاذ القانون المتخذة حيال تهديد ما، والتي قد تشمل احتجاز الفرد (أو الأفراد)، وإعاقة أنشطة الجهات المهددة (مثل إزالة المحتوى، وحجز الأصول)..<sup>5</sup></p>	<p><b>إجراءات إنفاذ القانون</b></p>
<p>يشير إلى القوانين المحلية، والأوامر التنفيذية أو القضائية، والتشريعات الإدارية، والسوابق القضائية، وغيرها من الأدوات أو المتطلبات القانونية الملزمة، بما في ذلك الالتزامات القانونية الناشئة عن القوانين الدولية والفقو وطنية حسب الساري في البلاد.</p>	<p><b>الإطار القانوني لوصول الحكومة إلى البيانات الشخصية</b></p>
<p>يتم تعريفها كـ "مجموعة من البيانات التي تصف وتقدم معلومات حول بيانات أخرى".</p>	<p><b>البيانات الوصفية</b></p>
<p>في حين يغطي مصطلح التكنولوجيات الجديدة مجموعة واسعة من التكنولوجيات المختلفة<sup>5</sup>، فإن التكنولوجيات الجديدة، ولأغراض هذا المستند، تشير إلى استخدام وسوء استخدام مثل هذه التكنولوجيات الجديدة كالإنترنت، ووسائل التواصل الاجتماعي، والعملات الرقمية المشفرة، والتعرف على الوجوه، والشبكة المظلمة<sup>6</sup>.</p>	<p><b>التكنولوجيات الجديدة</b></p>
<p>يشير إلى أي معلومات عبر الإنترنت تتعلق بشخص معرف أو يمكن تحديد هويته.</p>	<p><b>البيانات الشخصية على الإنترنت</b></p>
<p>في سياق العدالة الجنائية، يُستخدم مصطلح "إعادة التأهيل" للإشارة إلى التدخلات التي يديرها نظام الإصلاحات بهدف تغيير آراء الجاني أو سلوكه لتقليل احتمالية معاودة ارتكاب الجريمة، وتهيئة ودعم إعادة الاندماج في المجتمع.</p>	<p><b>إعادة التأهيل</b></p>
<p>عملية شاملة لإعادة إدماج الشخص في بيئة اجتماعية و/أو وظيفية.</p>	<p><b>إعادة الإدماج</b></p>
<p>المراقبة المنتظمة أو رصد الأفراد أو الجماعات أو الأنشطة من قبل جهة حكومية معتمدة، بما في ذلك جمع المعلومات وتسجيلها وتحليلها ونشرها، لغايات منع الجريمة والتحقيق فيها و/أو ملاحقة الأنشطة الإجرامية. قد يشمل ذلك المراقبة البدنية أو الإلكترونية (التنصت، أجهزة التعقب، الخ) أو الرقمية (تصفح الإنترنت، التواصل عبر البريد الإلكتروني، التفاعل على وسائل التواصل الاجتماعي).</p>	<p><b>المراقبة</b></p>

4 انظر على سبيل المثال قسم دليل النزاهة العامة لمنظمة التعاون الاقتصادي والتنمية 12.2.3. <https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en>

5 الذكاء الاصطناعي وإنترنت الأشياء وتقنيات البلوك تشين والأصول المشفرة والطائرات المسيرة والأنظمة الجوية المسيرة والحمض النووي وبصمات الأصابع وتكنولوجيا الفضاء الإلكتروني السيبرانية والتعرف على الوجه والطباعة ثلاثية الأبعاد.

6 التكنولوجيا لمكافحة الإرهاب، وثيقة البرنامج، الملحق الأول: توصيف الإجراءات.

عمليات إجرامية، بما في ذلك ضد المدنيين، ترتكب بنية التسبب بالموت أو الإصابة الجسدية الجسيمة، أو احتجاز الرهائن، بهدف إثارة حالة من الرعب بين العامة أو ضمن مجموعة من الأشخاص أو أشخاص معينين، وتخويف السكان أو إجبار الحكومة أو إحدى المنظمات الدولية على القيام أو الامتناع عن القيام بأي فعل، والذي يشكل جرائم ضمن نطاق الاتفاقيات والبروتوكولات الدولية المتعلقة بالإرهاب ووفق تعريفها<sup>7</sup>.

## ملخص تنفيذي

إن أكثر استجابات مكافحة الإرهاب فعالية هي تلك التي تتوافق مع التزامات حقوق الإنسان الدولية. فقد يترتب على سياسات الأمن القومي التدخلية أثر سلبي على احترام حقوق الإنسان وحمايتها، وبخاصة حقوق الخصوصية، وحرية التعبير والتجمع، وعدم التمييز. وسواء عبر الإنترنت أو خارجها، فإن ضمان توافق سياسات الأمن مع التزامات القانون الدولي يتطلب اعتماد الأطر القانونية الملائمة والمتوافقة مع حقوق الإنسان، وإنشاء آليات فعالة ومستقلة للشفافية والرقابة.

يركز هذا الدليل على التزامات الدول الأعضاء وليس على التزامات شركات تكنولوجيا المعلومات والاتصالات. حيث تُعالج مسؤوليات هذه الشركات المتعلقة بحقوق الإنسان في المبادئ التوجيهية للأمم المتحدة بشأن الأعمال التجارية وحقوق الإنسان<sup>8</sup>.

7 انظر قرار مجلس الأمن 1566 (2004)، الفقرة 3.

8 المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة "الحماية والاحترام والتعويض" المفوضية السامية لحقوق الإنسان.

# [أولا]

## خلفية

### 1 - 1 لمحة عامة

تولي الدول الأعضاء في الأمم المتحدة أهمية كبيرة لمعالجة تأثير التكنولوجيات الجديدة على مكافحة الإرهاب. خلال الاستعراض السابع لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب (A/RES/75/291)<sup>9</sup> في تموز/يوليه 2021، عبرت الدول الأعضاء عن قلقها العميق بشأن "استخدام الإنترنت وغيرها من تكنولوجيات المعلومات والاتصالات، بما في ذلك منصات التواصل الاجتماعي، لأغراض إرهابية، بما في ذلك الانتشار المستمر للمحتوى الإرهابي"، وطالبت مكتب الأمم المتحدة لمكافحة الإرهاب وغيره من الكيانات المنضوية تحت الميثاق العالمي لمكافحة الإرهاب "بالدعم المشترك للإجراءات والنهج المبتكرة بهدف بناء قدرة الدول الأعضاء، بناءً على طلبها، على التعامل مع التحديات والفرص التي توفرها التكنولوجيا الجديدة، بما في ذلك الجوانب المتعلقة بحقوق الإنسان، في منع الإرهاب ومكافحته". وتطالب قرارات مجلس الأمن رقم 2178 (2014)<sup>10</sup> ورقم 2396 (2017)<sup>11</sup> الدول الأعضاء بالتعاون عند اتخاذ إجراءات وطنية لمنع الإرهابيين من استغلال التكنولوجيا ووسائل الاتصال لأغراض إرهابية. كما يشجع قرار مجلس الأمن رقم 2396 (2017) الدول الأعضاء على تعزيز التعاون مع القطاع الخاص، خاصة مع شركات تكنولوجيا المعلومات والاتصالات، في جمع البيانات والأدلة الرقمية في قضايا تتعلق بالإرهاب.

أشار فريق الدعم التحليلي ورصد الجزاءات، في تقريره الثلاثين إلى مجلس الأمن التابع للأمم المتحدة<sup>12</sup>، إلى أن "كثيراً من الدول الأعضاء أبرزت الدور المتنامي لوسائل التواصل الاجتماعي وغيرها من التكنولوجيات عبر الإنترنت في تمويل الإرهاب ونشر الدعاية"، حيث ذكرت تلك الدول منصات مثل تيليجرام، ووكيت، تشات، هوب، وتامتام، من ضمن منصات أخرى. كما تمت الإشارة في التقرير إلى أن مؤيدي تنظيم الدولة الإسلامية (داعش) يستخدمون منصات على شبكة الإنترنت الخفية لتخزين المواد التدريبية والوصول إليها والتي ترفض مواقع أخرى استضافتها، بالإضافة إلى استخدامها للحصول على تكنولوجيات جديدة.

وتتم مناقشة مكافحة استخدام التكنولوجيات الجديدة والناشئة لأغراض إرهابية في الاجتماع الخاص المكرس للجنة مكافحة الإرهاب التابعة لمجلس الأمن في الأمم المتحدة، والمنعقد في 28-29 تشرين الأول/أكتوبر 2022 في نيودلهي، وأسفر عن اعتماد وثيقة غير ملزمة، تُعرف باسم إعلان نيودلهي<sup>13</sup>.

9 استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب: الاستعراض السابع (A/RES/75/291), N2117570.pdf (un.org)

10 قرار مجلس الأمن رقم 2178 (2014)، (undocs.org) S/RES/2178%20(2014)

11 قرار مجلس الأمن رقم 2396 (2017)، (undocs.org/S/RES/2396(2017)).http://undocs.org/S/RES/2396(2017)

12 التقرير الثلاثون لفريق الدعم التحليلي ورصد الجزاءات المقدم عملاً بالقرار 2610 (2021) بشأن تنظيم الدولة الإسلامية: (داعش) وتنظيم القاعدة وما يرتبط بهما من أفراد وجماعات ومؤسسات وكيانات (undocs.org) S/2022/547

13 إعلان دلهي، (undocs.org) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc\_special\_meeting\_outcome\_document.pdf

أشارت اللجنة إلى "قلقها حيال الاستخدام المتزايد، من قبل الإرهابيين وأنصارهم، في مجتمع عالمي، لشبكة الإنترنت وتقنيات المعلومات والاتصالات الأخرى، بما في ذلك منصات وسائل التواصل الاجتماعي، لأغراض إرهابية"، وأقرت "بضرورة تحقيق توازن بين تعزيز الابتكار ومنع ومكافحة استخدام التكنولوجيات الجديدة والناشئة، مع اتساع تطبيقها، لأغراض إرهابية"، مؤكدة "ضرورة الحفاظ على الاتصال العالمي والحركة الحرة والأمن للمعلومات بما ييسر التنمية الاقتصادية، والتواصل، والمشاركة والوصول إلى المعلومات".

## 1 - 2 مبادرة التكنولوجيا لمكافحة الإرهاب

مبادرة التكنولوجيا لمكافحة الإرهاب هي مبادرة مشتركة بين منظمة الإنتربول ومكتب الأمم المتحدة لمكافحة الإرهاب/مركز الأمم المتحدة لمكافحة الإرهاب، تم تنفيذها ضمن برنامج الأمم المتحدة العالمي لمكافحة الإرهاب حول أمن الفضاء الإلكتروني والتكنولوجيات الجديدة. وتهدف إلى تعزيز قدرات سلطات إنفاذ القانون والعدالة الجنائية في الدول الشريكة المحددة لمواجهة استغلال التكنولوجيات الجديدة والناشئة لأغراض إرهابية، بالإضافة إلى دعم وكالات إنفاذ القانون في الدول الشريكة في الاستفادة من التكنولوجيات الجديدة والناشئة في مكافحة الإرهاب.

### الشكل 1

تعزيز قدرات أجهزة إنفاذ القانون وسلطات العدالة الجنائية في مواجهة استغلال التكنولوجيا الجديدة والناشئة لأغراض إرهابية ودعم توظيف التكنولوجيا الجديدة والناشئة في مكافحة الإرهاب كجزء من هذا الجهد.



ولتحقيق الهدف العام، تطبق مبادرة التكنولوجيا لمكافحة الإرهاب نتيجتين بارزتين مع ستة مخرجات أساسية.

## الجدول 1 - النتائج والمخرجات لمبادرة التكنولوجيا لمكافحة الإرهاب

**النتيجة 1:** استجابات سياسية فعالة لمكافحة الإرهاب تجاه التحديات والفرص المتعلقة باستخدام التكنولوجيا الجديدة في مكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

تطوير المنتجات المعرفية لتصميم استجابات السياسات الوطنية لمكافحة الإرهاب للتصدي للتحديات والفرص التي توفرها التكنولوجيات الجديدة في مكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.



المخرج 1 - 1

زيادة الوعي والمعرفة بالممارسات الجيدة بشأن تحديد المخاطر والفوائد المرتبطة بالتكنولوجيات الجديدة والإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.



المخرج 2 - 1

زيادة قدرات دول شريكة محددة على تطوير استجابات سياسية وطنية فعالة لمكافحة الإرهاب من أجل مكافحة استخدام الإرهابيين للتكنولوجيات الجديدة والاستفادة من هذه التكنولوجيات الجديدة لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.



المخرج 3 - 1

**النتيجة 2:** زيادة القدرة التشغيلية لأجهزة إنفاذ القانون والعدالة الجنائية في مواجهة استغلال التكنولوجيا الجديدة لأغراض إرهابية واستخدام التكنولوجيا الجديدة لمنع الإرهاب ومكافحته مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

تطوير أدوات وإرشادات عملية لإنفاذ القانون بشأن مكافحة استغلال التكنولوجيات الجديدة لأغراض إرهابية واستخدام هذه التكنولوجيات الجديدة لمنع الإرهاب ومكافحته مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.



المخرج 1 - 2

تعزيز مهارات مؤسسات إنفاذ القانون والعدالة الجنائية في الدول الشريكة لمكافحة استغلال التكنولوجيات الجديدة لأغراض إرهابية واستخدام هذه التكنولوجيات الجديدة لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.



المخرج 2 - 2

زيادة التعاون وتبادل المعلومات بين أجهزة الشرطة الدولية بشأن مكافحة استخدام الإرهابيين للتكنولوجيات الجديدة واستخدام هذه التكنولوجيات الجديدة لمكافحة الإرهاب.



المخرج 3 - 2

## 3 - 1 أغراض الوثيقة واستخداماتها

تهدف هذه الوثيقة إلى توجيه عملية تأسيس آليات مستقلة وفعالة للشفافية والرقابة من أجل مراقبة الإنترنت وجمع البيانات المتعلقة بمكافحة الإرهاب عبر الإنترنت.

### 1 - 3 - 1 النطاق

تهدف هذه الوثيقة إلى نشر الوعي بشأن المخاوف المتعلقة بحقوق الإنسان والخصوصية في ممارسات جمع البيانات عبر الإنترنت لأغراض إنفاذ قوانين مكافحة الإرهاب، كما تعرض الاعتبارات الرئيسية في الرقابة لضمان وضع الإجراءات الوقائية المناسبة ضمن ممارسات جمع البيانات عبر الإنترنت فيما يتعلق بالمعايير والممارسات الدولية لحقوق الإنسان.

### 1 - 3 - 2 الجمهور المستهدف

تم تصميم هذا الدليل بشكل أساسي لصناع السياسات، على الرغم من أن يكون وكالات إنفاذ القانون يجب أن تكون على دراية بمبادئه الرئيسية والآليات المتصلة.

### 1 - 3 - 3 الفوائد

يحفل التاريخ بأمثلة عديدة على الاستجابة للتهديدات الإرهابية بطرق أدت إلى خلق أو تضخيم المظالم القائمة والتي قد تشجع بدورها على تعزيز الإرهاب والتطرف العنيف المؤدي إلى الإرهاب. تسهم الآليات المستقلة الفعالة للرقابة في زيادة المساءلة والشفافية.

### 1 - 3 - 4 أوجه القصور

لا يعالج هذا الدليل بعمق العديد من المخاوف المتعلقة بشراء البيانات الشخصية المجموعة تجاريا من قبل الوكالات الحكومية، على الرغم من أن هذه الممارسة تثير قضايا كبيرة حول الخصوصية. كما أنه لا يعالج الرقابة على القطاع الخاص.



# [ثانياً]

## النهج

### 2 - 1 ملحة عامة

يسعى التقرير إلى دعم وتمكين الدول الأعضاء لتعزيز الامتثال للمعايير والمبادئ الدولية لحقوق الإنسان في الاستفادة من التقنيات الجديدة لمنع ومكافحة الإرهاب، مع التركيز على إنشاء آليات شفافة ومستقلة لمراقبة وجمع البيانات عبر الإنترنت المتعلقة بمكافحة الإرهاب. كما يسعى إلى دعم وتمكين الدول الأعضاء لإجراء تقييمات فعالة للتهديد في مجال مكافحة استخدام التكنولوجيات الجديدة لأغراض إرهابية، والتي تتماشى مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب مع الاحترام الكامل لحقوق الإنسان وسيادة القانون.

### 2 - 2 الإطار التوجيهي

#### الشكل 2



يعتبر الإطار التوجيهي نموذجاً مفاهيمياً يهدف إلى توجيه تطوير التقرير ومواءمته وإثرائه. ويسعى لضمان الترابط، بداية من الاستراتيجية حتى التنفيذ، بين استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب وأهداف السياسات والاستراتيجية الوطنية لمكافحة الإرهاب في الدول الأعضاء ونتائجها وخدماتها وقدراتها من منظور إنفاذ القانون والعدالة الجنائية، فيما يتعلق بالتكنولوجيات الجديدة. تحدد استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب، التي اعتمدها الجمعية العامة، إجراءات واسعة للدول الأعضاء لمواجهة التهديدات الإرهابية، والتي تندرج تحت أربع ركائز رئيسية:

**الركيزة الأولى:** إجراءات لمعالجة الظروف المؤدية إلى انتشار الإرهاب

**الركيزة الثانية:** إجراءات للحد من الإرهاب ومكافحته

**الركيزة الثالثة:** الإجراءات الرامية إلى بناء قدرة الدول على الحد من الإرهاب ومكافحته وتعزيز دور منظومة الأمم المتحدة في هذا الصدد

**الركيزة الرابعة:** الإجراءات الرامية إلى ضمان احترام حقوق الإنسان للجميع وسيادة القانون كأساس جوهري في مكافحة الإرهاب

يتم تشجيع الدول الأعضاء على تطوير أطرها الوطنية القانونية والسياسية لمكافحة الإرهاب بما يتماشى مع استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب. حيث يجب عليها أن تضمن توافق قوانينها وسياساتها واستراتيجياتها وإجراءاتها في مكافحة الإرهاب مع التزاماتها بموجب القانون الدولي، بما في ذلك القانون الدولي لحقوق الإنسان، والقانون الدولي للاجئين، والقانون الإنساني الدولي. وينبغي لأطر القوانين والسياسات الوطنية لمكافحة الإرهاب في الدولة العضو أن تسعى عموماً لمنع التطرف العنيف الذي قد يؤدي إلى الإرهاب ومعالجته، ومنع الأنشطة الإرهابية أو تقييدها، واتخاذ الإجراءات الملائمة لحماية الأشخاص الخاضعين لسلطة الدولة والخدمات والبنية التحتية من تهديد الهجمات الإرهابية المتوقعة بشكل معقول، وضمان محاسبة الإرهابيين على أفعالهم.

ولتحقيق النتائج والأهداف في مجال مكافحة الإرهاب، تمتلك سلطات إنفاذ القانون والعدالة الجنائية الوطنية في الدول الأعضاء مجموعة من الأدوات تحت تصرفها. تشمل ما يلي على سبيل المثال لا الحصر:



## الجدول 2 - خدمات إنفاذ القانون والعدالة الجنائية الوطنية الرفيعة المستوى في مكافحة الإرهاب

الخدمات	الوصف
إجراءات العدالة الجنائية	هي إجراءات قانونية لتوجيه تهم الإرهاب لفرد أو كيان وجلسة المحكمة والحكم أو القرار والعقوبة وكذلك الإصلاح وإعادة التأهيل.
الاستخبارات الجنائية	هي ناتج جمع المعلومات ومعالجتها ونشرها وتحليلها وتفسيرها والتي جمعت من مصادر متعددة، بهدف إفادة صناع القرار لأغراض التخطيط لاتخاذ القرارات أو الإجراءات - على المستوى الاستراتيجي أو التشغيلي أو التكتيكي. يجب جمع الاستخبارات وحفظها واستخدامها ومشاركتها وفقاً للالتزامات الدول الأعضاء المعنية بموجب القانون الدولي لحقوق الإنسان.
التحقيقات الجنائية	هي عملية جمع المعلومات (أو الأدلة) لتقرير ارتكاب الجريمة من عدمه، وتحديد الجاني وتقديم الأدلة التي تدعم إجراءات العدالة الجنائية.
إجراءات إنفاذ القانون	تصف عادة إجراءات إنفاذ القانون المتخذة حيال تهديد ما، والتي قد تشمل احتجاز الفرد (أو الأفراد)، وإعاقة أنشطة الجهات المهددة (مثل إزالة المحتوى، وحجز الأصول) .. إلخ.
إعادة التأهيل	في سياق العدالة الجنائية، يُستخدم مصطلح "إعادة التأهيل" للإشارة إلى التدخلات التي يديرها نظام الإصلاحات بهدف تغيير آراء الجاني أو سلوكه لتقليل احتمالية معاودة ارتكاب الجريمة، وتهيئة ودعم إعادة الاندماج في المجتمع.
إعادة الإدماج	عملية شاملة لإعادة إدماج الشخص في بيئة اجتماعية و/أو وظيفية.

يعتمد الاستخدام والنشر الفعال لمثل هذه الخدمات والأدوات على مجموعة من القدرات الأساسية. ويتم غالباً تعريف القدرات المطلوبة لتمكين الخدمات وتقديمها وعرضها ضمن نموذج القدرات. حيث يمثل نموذج القدرات تحليلاً وظيفياً للوظائف الرئيسية إلى مجموعات منطقية ومتناهية الصغر تدعم تنفيذ الخدمات والأنشطة. ويوضح نموذج القدرات المتطلبات من الأشخاص (الهيكل التنظيمي والمهارات) والعمليات والتكنولوجيا والبنية التحتية والتمويل.

ويعمل الإطار التوجيهي على ضمان التوافق بين الاستراتيجية والتنفيذ في كلا الاتجاهين "التنازلي" و "التصاعدي".

## 2 - 3 المنهجية

### الشكل 3



تتضمن منهجية تطوير هذه الوثيقة حول "إنشاء الأطار التشريعي وآليات الشفافية والرقابة لجمع البيانات عبر الإنترنت" البحث والتحليل، والتشاور مع أصحاب المصلحة والخبراء المعنيين، وتشمل وثائق مشروع تكنولوجيا مكافحة الإرهاب، والتشاور مع أصحاب المصلحة، والتحليل الداخلي، والأبحاث المكتبية، واجتماعات مجموعات الخبراء، والتنسيق مع كيانات اتفاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب، والإطار التوجيهي الوارد أعلاه في القسم 2 - 2. وبناء على هذه الأنشطة، تحدد المخرجات الرئيسية لهذه الوثيقة القضايا الرئيسية المتعلقة بحقوق الإنسان والخصوصية والتحديات فيما يتعلق بجمع البيانات عبر الإنترنت، كما تعرض الاعتبارات الرئيسية للرقابة من خلال الآليات التشريعية وآليات الشفافية.

## 2 - 3 - 1 اجتماعات ومشاورات فريق الخبراء

تم تطوير هذا الدليل بمشاركة الخبراء من خلال جلسات اجتماع فريق الخبراء بالإضافة إلى استشارات ومراجعات فردية. جمع اجتماع فريق الخبراء بين مجموعة من الخبراء والممارسين من وكالات مكافحة الإرهاب وإنفاذ القانون، وحقوق الإنسان، والقطاع الخاص، والجهات الأكاديمية، والمجتمع المدني، لمناقشة طرق مواجهة استخدام التكنولوجيات الجديدة لأغراض إرهابية وتوظيف هذه التكنولوجيات كجزء من هذا الجهد، وتحديد الممارسات الجيدة في هذا الصدد، إضافة إلى مناقشة المخاطر والتحديات والممارسات غير الجيدة التي تتطلب التنبه والحد. وقد خضع الدليل لمزيد من التشذيب بمشاركة ميثاق الأمم المتحدة العالمي لتنسيق مكافحة الإرهاب ومجموعته العاملة في مواجهة التهديدات الناشئة وحماية البنية التحتية الحيوية، والتي تعمل على تعزيز التنسيق والترابط لدعم جهود الدول الأعضاء في منع التهديدات الإرهابية الناشئة والاستجابة لها، مع احترام حقوق الإنسان وسيادة القانون كأساس جوهري، بالتوافق مع القانون الدولي، بما في ذلك حقوق الإنسان والقانون الإنساني وقانون اللاجئين.

## 2 - 3 - 1 مراجعة الوثيقة المرجعية

تم تطوير هذا الدليل بناءً على الأبحاث والأدلة الإرشادية والمنشورات الحالية وتم أخذها في الاعتبار والبناء عليها واستكمالها، وتتضمن ما يلي:

الجدول 3 - المراجع	
1	استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب.
2	تقارير المفوضية السامية للأمم المتحدة لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي.
3	تقرير مارتن شاينين، المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب. مجموعة من الممارسات الجيدة بشأن الأطر والإجراءات القانونية والمؤسسية التي تضمن احترام وكالات الاستخبارات لحقوق الإنسان في سياق مكافحة الإرهاب، بما في ذلك احترامها للرقابة.
4	حالة التعاون الدولي من أجل الوصول القانوني إلى الأدلة الرقمية: وجهات نظر بحثية، تقرير اتجاهات المديرية التنفيذية للجنة مكافحة الإرهاب، كانون الثاني/يناير 2022.
5	مبادئ تشواني بشأن الأمن القومي والحق في الحصول على المعلومات.
6	مكتب الأمم المتحدة المعني بالمخدرات والجريمة، دليل مساءلة الشرطة والرقابة والنزاهة.
7	دليل النزاهة العامة لمنظمة التعاون الاقتصادي والتنمية.
8	مجلس أوروبا، دليل عملي حول استخدام البيانات الشخصية في قطاع الشرطة.
9	تقرير فرانك لارو، المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير A/HRC/23/40.

# [ثالثاً]

## مقدمة

### 3 - 1 ملحة عامة

مع استمرار التقدم في التكنولوجيا، يقوم الإرهابيون باستغلال هذه الابتكارات بشكل متزايد لتعزيز أجداتهم التدميرية. ويشكل استغلال الإرهاب للانتشار السريع لمنصات الاتصال، وشبكات التواصل الاجتماعي، وتكنولوجيات التشفير والرميز، والتكنولوجيات الناشئة، تحديات جمة أمام سلطات إنفاذ القانون. إن دمج التكنولوجيا في ترسانة الجماعات الإرهابية يفرض تحديات غير مسبوقة، مما يتطلب من الحكومات إعادة تقييم استراتيجياتها وتكييف أساليبها.

يجب على الدول الأعضاء، عند وضع سياسات مكافحة الإرهاب، إدراك الحاجة الملحة لفهم استغلال الإرهابيين للتكنولوجيات الناشئة وتوقعه والتصدي له بفعالية. تركز هذه السياسات على مجموعة من الجوانب، بما في ذلك الوعي، وتدخلات التهديد، والقدرات الوطنية في مجال مكافحة الإرهاب، والتعاون، ومبادرات بناء القدرات. وتهدف الحكومات، من خلال اعتماد سياسات شاملة ومرنة ومتوافقة مع حقوق الإنسان في مجال مكافحة الإرهاب على الصعيد الوطني، إلى الحفاظ على موقع متقدم، والتخفيف بشكل استباقي من المخاطر المرتبطة باستغلال الإرهابيين للتكنولوجيا الجديدة مع مراعاة حماية الأمن وحقوق الأفراد ضمن سلطاتها، بما في ذلك الحق في الخصوصية.

### 3 - 2 التكنولوجيات الجديدة ومكافحة الإرهاب

يقود التقدم في التكنولوجيا الرقمية والبيانات وشبكة الإنترنت اليوم إلى عالم شديد الترابط، حيث يمكن الوصول إلى المعلومات ومشاركتها واستلامها بصورة لحظية تقريباً. حيث كان ما يقرب من 70 في المائة من سكان العالم يستخدمون الإنترنت بحلول عام 2022<sup>14</sup>، أكثر من 93 في المائة هم من مستخدمي وسائل التواصل الاجتماعي<sup>15</sup>. ويُقدر عالمياً أنه قد تم إنشاء أكثر من 97 زيتابايت<sup>16</sup> من المعلومات في عام 2022<sup>17</sup>. وفي حين توفر مثل هذه التكنولوجيات فرصة لتحويل المجتمع نحو الصالح العام، فإن الجهات الإرهابية تستغل هذه التكنولوجيا لأغراضها الشنيعة، حيث يفرض استخدام التكنولوجيات الجديدة لأغراض إرهابية تحديات كبيرة أمام الدول الأعضاء في التصدي للإرهاب، وخاصة عند استخدام تكنولوجيات تسمح بإخفاء الهوية والقدرة على التنسيق والعمل عن بُعد.

14 تقرير التواصل العالمي للاتحاد الدولي للاتصالات 2022، <https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/>

15 بيانات دومو لا تنام أبداً، Domo | Data Never Sleeps 10.0.

16 الزيتابايت يساوي مليار ترابايت.

17 ستاتيسستا، Total data volume worldwide 2010-2025 | Statista.

من ناحية أخرى، تتيح التكنولوجيات الجديدة فرصاً كبيرة كعامل مضاعف لقدرات سلطات إنفاذ القانون ومكافحة الإرهاب. على سبيل المثال، يمكن لهذه التكنولوجيات أن تتيح لسلطات إنفاذ القانون القيام بالمزيد باستخدام موارد أقل، وتسريع اتخاذ القرارات في الوقت المناسب، وتوليد رؤى جديدة، وإجراء عمليات التعطيل عن بُعد. في الوقت نفسه، تثار مخاوف بشأن المخاطر على الخصوصية وممارسة حقوق الإنسان بشكل عام، الناجمة عن التشريعات ذات الصلة التي تسمح باستخدام مثل هذه التقنيات، والتي غالباً ما تكون دون المعايير الدولية لحقوق الإنسان المعمول بها، وكذلك من تطبيقها من قبل أجهزة إنفاذ القانون.

وتتوقف مكافحة استخدام الجهات الإرهابية للتكنولوجيات الجديدة على فهم طريقة استخدام الجهات الإرهابية لهذه التكنولوجيات، وتطوير إطار قانوني واستجابات سياسية فعّالة، وبناء القدرة التشغيلية للتصدي لاستخدام مثل هذه التكنولوجيات لأغراض إرهابية، بما في ذلك توظيف التكنولوجيات الجديدة واعتمادها.

### 3 - 2 - 1 - التحديات - استخدام التكنولوجيات الجديدة لأغراض إرهابية

إن التقدم في تكنولوجيا المعلومات والاتصالات وتوافرها جعلها مغرية للجماعات الإرهابية وجماعات التطرف العنيف لاستغلال الإنترنت ووسائل التواصل الاجتماعي في تيسير مجموعة واسعة من الأنشطة، بما في ذلك التحريض، والتطرف، والتجنيد، والتدريب، والتخطيط، وجمع المعلومات، والتواصل، والتضخيم، والترويج، والتمويل. كما يستخدم الإرهابيون الاتصالات المشفرة والشبكة المظلمة لمشاركة المحتوى الإرهابي والخبرات، مثل تصاميم الأجهزة المتفجرة المرتجلة واستراتيجيات الهجوم، وكذلك لتنسيق الهجمات وتيسيرها وتوفير الأسلحة والوثائق المزورة. وفي الوقت ذاته قد تعني التطورات في مجالات الذكاء الاصطناعي والتعلم الآلي والجيل الخامس من الاتصالات والروبوتات والبيانات الضخمة والمرشحات الخوارزمية والتكنولوجيا الحيوية والسيارات الذاتية القيادة والطائرات بدون طيار أنه عندما تصبح هذه التكنولوجيات متوفرة تجارياً وميسورة التكلفة وسهلة الاستخدام، قد يستغلها الإرهابيون أيضاً لتوسيع نطاق هجماتهم وخطورتها.

### 3 - 2 - 2 - الفرص - إنفاذ القانون في مكافحة الإرهاب

توفر التكنولوجيات الجديدة فرصاً لا حصر لها لوكالات إنفاذ القانون لمكافحة الإرهاب بفاعلية، مع الحفاظ على ممارسات مسؤولة تجاه القوانين الدولية لحقوق الإنسان. يمكن لسلطات إنفاذ القانون توظيف التكنولوجيات الجديدة لاكتشاف الأنشطة الإرهابية والتحقيق فيها وملاحقتها قضائياً ومحاكمتها بطرق جديدة أكثر فاعلية.

تسمح استخبارات المصادر المفتوحة بالجمع السريع للمعلومات حول الأهداف المعنية، مما يجعل أنشطة إنفاذ القانون أكثر فاعلية. وتتيح قدرات تحليل البيانات المتقدمة والذكاء الاصطناعي معالجة كميات هائلة من المعلومات وتحليلها، مما يمكن أجهزة إنفاذ القانون من تحديد الأنماط وكشف التهديدات المحتملة والاستجابة الاستباقية لأنشطة الإرهاب. كما تساعد نظم المراقبة المتقدمة، بما في ذلك التعرف على الوجوه والتكنولوجيات البيومترية، في التعرف على المشتبه بهم وتتبعهم، مما يعزز كفاءة التحقيقات ومنع الهجمات المحتملة وملاحقة الإرهابيين. علاوة على ذلك، تساعد أدوات التحليل الجنائي الرقمية في استخراج الأدلة الحاسمة من الأجهزة الإلكترونية، مما يمكن أجهزة إنفاذ القانون من كشف الروابط الخفية وتعطيل الشبكات الإرهابية ومحاكمة الإرهابيين.

يمكن أن يساهم استغلال التكنولوجيات الجديدة في تحديد أولويات موارد إنفاذ القانون المحدودة بطريقة أكثر فاعلية. ولكن من الأهمية بمكان أن توظف هذه التكنولوجيات بشكل أخلاقي مع الامتثال الصارم للخصوصية وحقوق الإنسان وسيادة القانون. ويجب تطبيق إجراءات الشفافية والمساءلة لضمان الاستخدام المسؤول ومنع أي إساءة استخدام محتملة لهذه الأدوات القوية. كما يجب إجراء برامج تدريب شاملة لتزويد موظفي إنفاذ القانون بالمهارات اللازمة لتوظيف التكنولوجيات الجديدة بشكل فعال لا يتجاوز حدود الأطر القانونية والأخلاقية. يمكن لأجهزة إنفاذ القانون من خلال استغلال التكنولوجيا الجديدة بشكل مسؤول، تعزيز جهودها في مجال مكافحة الإرهاب وحماية أمن المجتمعات وسلامتها.

### 3 - 2 - 3 حقوق الإنسان والتكنولوجيات الجديدة

يمثل الإرهاب تحدياً خطيراً لمبادئ حكم القانون بذاتها، ولحماية حقوق الإنسان، وتطبيقها بشكل فعال. حيث يمكن للإرهاب أن يؤدي إلى زعزعة استقرار الحكومات المشكلة بشكل شرعي، وتقويض دعائم المجتمع المدني المتعدد الأطياف، وتهديد الأمن والسلام، وتعريض التنمية الاجتماعية والاقتصادية للخطر. وتحمل الدول مسؤولية اتخاذ الإجراءات المناسبة لحماية الأفراد الخاضعين لسيادتها من تهديد الهجمات الإرهابية المتوقعة بشكل معقول. ويشمل واجب الدول في حماية حقوق الإنسان الالتزام باتخاذ الإجراءات اللازمة والكافية لمنع الأنشطة التي تعرض هذه الحقوق للخطر ومحاربتها والمعاقبة عليها، كالتهديدات الموجهة للأمن القومي أو الجرائم العنيفة، بما في ذلك الإرهاب. ويجب أن تتوافق جميع هذه الإجراءات بذاتها مع القوانين الدولية لحقوق الإنسان ومعايير سيادة القانون.

وفي سياق استخدام التكنولوجيات الجديدة لمكافحة الأنشطة الإرهابية، يجب على الدول ضمان احترام القوانين والسياسات والممارسات المعنية للحقوق: كحق الخصوصية، وحق حرية التعبير وحرية التجمع، وحرية الفكر والوجدان والدين، وحق الفرد في الحرية والأمن، وحق الحصول على محاكمة عادلة بما في ذلك قرينة البراءة، ومبدأ عدم التمييز. كما يجب أن تلتزم الدول أيضاً بمنع التعذيب والمعاملة القاسية أو اللاإنسانية أو المهينة منعاً قاطعاً.

وقد أكدت كل من الأمم المتحدة والانتربول والاتحاد الأوروبي مراراً وتكراراً على الارتباط المتبادل بين التكنولوجيات الجديدة ومكافحة الإرهاب وحقوق الإنسان، بما في ذلك المساواة بين الجنسين. وتسلط استراتيجيات الأمم المتحدة العالمية لمكافحة الإرهاب ومختلف قرارات الجمعية العامة ومجلس الأمن الضوء على التزامات الدول الأعضاء في إطار القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي والقانون الدولي للاجئين عند مكافحة الإرهاب. وتقر استراتيجيات الأمم المتحدة لمكافحة الإرهاب، على وجه الخصوص، بأن "إجراءات مكافحة الإرهاب الفعالة وحماية حقوق الإنسان ليست أهدافاً متعارضة، بل هي متكاملة وتعزز بعضها البعض" وتتطلب إجراءات لضمان احترام حقوق الإنسان للجميع وسيادة القانون كأساس جوهري للحرب ضد الإرهاب. وبشكل خاص، شجعت الاستراتيجيات الدولية الأعضاء على معالجة استخدام الإنترنت وغيرها من تكنولوجيا المعلومات والاتصالات، ومنها منصات التواصل الاجتماعي، لأغراض إرهابية، بما في ذلك استمرار انتشار المحتوى الإرهابي، مع احترام القانون الدولي، متضمناً القانون الدولي لحقوق الإنسان، وحق حرية التعبير.

### 3 - 2 - 4 النوع الاجتماعي والتكنولوجيا وتقييم التهديدات

يشير النوع الاجتماعي إلى الأدوار والسلوكيات والأنشطة والصفات التي تعتبرها المجتمعات المختلفة، في فترة زمنية معينة، ملائمة للرجال والنساء والفتيات والفتيات. بالإضافة إلى الصفات والفرص الاجتماعية المرتبطة بكون الإنسان ذكراً أو أنثى، يرتبط النوع الاجتماعي أيضاً بالعلاقات بين النساء والرجال والفتيات والفتيات. ويشكل النوع الاجتماعي جزءاً من السياق الاجتماعي الثقافي الأوسع، ويتقاطع مع عوامل الهوية الأخرى، بما في ذلك الجنس والطبقة الاجتماعية والعرق ومستوى الفقر والإثنية والتوجه الجنسي والعمر، من ضمن عوامل أخرى. ويختبر الرجال والنساء والفتيات والفتيات، وكذلك الأشخاص ذوو الهوية الجنسية أو التعبير الجنسي المختلف، يختبرون الأمن بطرق مختلفة وفقاً لاحتياجاتهم وجوانب ضعفهم وقدراتهم الخاصة<sup>18</sup>. ومع أن استخدام التكنولوجيات الجديدة تحدياً يمكن أن يترافق مع غياب البنى الهيكلية الهرمية على الإنترنت الأمر الذي يزيل القيود المتعلقة بالنوع الاجتماعي، ويوفر فرصاً لتمكين النساء، لكنه من جهة أخرى يزيد من احتمالية تجنيدهن أو مشاركتهن النشطة في مجموعات التطرف العنيفة أو المجموعات الإرهابية عبر الإنترنت<sup>19</sup>. كما تشير الأدلة إلى أن المجموعات الإرهابية تستغل عدم المساواة بين الجنسين، والعادات والأعراف والأدوار ومفاهيم الرجولة وغيرها وذلك لأغراضها الخاصة بها في رسائلها عبر الإنترنت؛ على سبيل المثال، أستطاع تنظيم "داعش" براءة تجنيد نساء من خلال وسائل التواصل الاجتماعي، حيث قام التنظيم بتغيير خطابه وفقاً لجمهوره المستهدف، ليتناسب مع مجموعة متنوعة من النساء اللواتي يتحدثن لغات مختلفة، ويعشن في مناطق وسياقات اجتماعية واقتصادية

18 مركز جنيف للرقابة الديمقراطية على القوات المسلحة، ومنظمة الأمن والتعاون في أوروبا/ مكتب المؤسسات الديمقراطية وحقوق الإنسان، وهيئة الأمم المتحدة للمرأة، مجموعة أدوات النوع الاجتماعي وإصلاح قطاع الأمن (جنيف: مركز جنيف للرقابة الديمقراطية على القوات المسلحة، 2008). <https://www.dcaf.ch/gender-and-security-toolkit>

19 المديرية التنفيذية للجنة مكافحة الإرهاب، "الأبعاد الجنسانية للرد على المقاتلين الإرهابيين الأجانب العائدين - وجهات نظر بحثية"، شباط/فبراير 2019.

وثقافية مختلفة في غرب أوروبا، ووسط آسيا، والشرق الأوسط وشمال أفريقيا، مستفيداً من عدم المساواة بين الجنسين في محاولته للتأثير على الجمهور المستهدف. يتمثل أحد الجوانب المهمة الأخرى المتعلقة بالنوع الاجتماعي والتكنولوجيات الجديدة في الفجوة الرقمية بين الجنسين، حيث تقدر إمكانية وصول النساء إلى الإنترنت عالمياً بـ 85 في المائة من إمكانية وصول الرجال، بوجود عدد تقديري يبلغ نحو 1,7 مليار امرأة في الجنوب العالمي محرومة من فرصة الوصول إلى الإنترنت. تشكل هذه الفجوة قلقاً حول حقوق الإنسان يكمن في جميع جوانب أمن الفضاء الإلكتروني، بما في ذلك التعرض المحتمل للمخاطر وعدم الأمان أو المشاركة في الإدارة<sup>20</sup>.

---

20 مركز جنيف للرقابة الديمقراطية على القوات المسلحة، "المساواة بين الجنسين والأمن السيبراني وحوكمة قطاع الأمن - فهم دور النوع الاجتماعي في إدارة الأمن السيبراني"، كانون الثاني/يناير 2023.

## [رابعاً]

# جمع البيانات عبر الإنترنت من قبل سلطات إنفاذ القانون

### 4 - 1 ملحة عامة

مع تسارع التطورات التكنولوجية، يستغل الإرهابيون بشكل متزايد منصات الاتصال وشبكات التواصل الاجتماعي وتقنيات التشفير، وغيرها من التكنولوجيات الجديدة والناشئة لتجنيد الأعضاء وتنظيمهم، والحصول على الأسلحة، وتمويل العمليات، وكذلك من أجل التخطيط للعمليات الإرهابية ودعمها وارتكابها والتستر عليها. في الوقت ذاته، توفر هذه التقنيات نفسها أدوات جديدة لإجراءات إنفاذ القانون تساعد في تحديد الإرهابيين المشتبهين المحتملين، ومراقبة عضوية الكيانات الإرهابية، ورصد أنشطتهم، وعرقلة عملياتهم. مع ذلك، وفي حين تيسر التكنولوجيا الجديدة عمليات التعرف والمراقبة والسيطرة، فإن التهديدات للحقوق الأساسية، بما في ذلك حقوق الخصوصية، وحرية التعبير والتجمع، والحق في عدم التمييز، قد تزايدت، وكثيراً ما تتم إساءة استخدام قواعد الأمن القومي لتبرير جمع البيانات الترخلي عبر الإنترنت. وعلى الرغم من أن التكنولوجيات المعنية قد تكون جديدة، إلا أن المخاطر المرتبطة بالمراقبة غير المنظمة ليست كذلك. فقد ذكرت المحكمة الأوروبية لحقوق الإنسان بالفعل في عام 1978 أن "إدراك المحكمة للخطر الذي تشكله المراقبة غير المنظمة على تقويض الديمقراطية أو حتى إتلافها تحت مسمى الدفاع عنها، يؤكد أنه [...] لا يجوز للدول أن تتخذ أي إجراءات تراها مناسبة، باسم مكافحة التجسس والإرهاب"<sup>21</sup>. وبالمثل، تقرر استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب "بأن الإجراءات الفعالة لمكافحة الإرهاب وحماية حقوق الإنسان ليست أهدافاً متضاربة، بل متكاملة ومتعاضة"<sup>22</sup>. ومع ذلك، تشارك الدول الأعضاء بشكل منتظم في المراقبة الإلكترونية والرقمية لممثلي المجتمع المدني والصحفيين والأشخاص الذين يختلفون ببساطة في الرأي مع حكوماتهم، وتستخدم المعلومات المجموعة لاستهدافهم وقمعهم وإسكاتهم تحت غطاء الأمن القومي.

رداً على المخاوف المتزايدة بشأن التسارع السريع للرقابة الحكومية الميسرة بواسطة التكنولوجيا الجديدة، اعتمدت الجمعية العامة القرار 179/73، الذي يؤكد الحق في الخصوصية ويدعو الدول إلى "إنشاء أو الحفاظ على آليات مستقلة وفعالة ومزودة بمصادر كافية ونزيهة للرقابة الداخلية القضائية و/أو الإدارية و/أو البرلمانية تكون قادرة على ضمان الشفافية، كما يلزم، ومساءلة عمليات مراقبة الدولة للاتصالات واعتراضها وجمع البيانات الشخصية"<sup>23</sup>. وقد تكررت مبادئ الرقابة الفعالة والتعويض المناسب، بما في ذلك من خلال المراجعة القضائية وغيرها من السبل القانونية، في المراجعات السابعة والثامنة لاستراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب<sup>24</sup>.

21 المحكمة الأوروبية لحقوق الإنسان، كلاس وآخرون ضد ألمانيا، رقم 71/5029، 6 أيلول/سبتمبر 1978، الفقرة 49.

22 القرار A/RES/60/288، فقرة الديباجة حتى العمود الرابع.

23 القرار A/RES/73/179، الفقرة 6 (د).

24 القرار A/RES/75/291، الفقرة 106 (المراجعة السابعة)، القرار A/RES/77/298، الفقرة 110 (المراجعة الثامنة).

يجب أن تتضمن الممارسات والآليات المثلى: إرشادات داخلية واضحة ودقيقة للوصول لسلطات إنفاذ القانون إلى البيانات عبر الإنترنت يزود بها الضباط المعنيون قبل الوصول إلى أية بيانات شخصية؛ والإشراف الداخلي على جمع البيانات أثناء العمليات؛ والتحويل المسبق المستقل لجمع أنواع معينة من المعلومات؛ والرقابة المستقلة على عمليات إنفاذ القانون أثناء العمليات وبعدها؛ والوصول إلى آليات التعويض وتوفير الجزاءات الفعالة وإلى ضحايا انتهاكات حقوق الإنسان.

## 4 - 2 المصطلحات: جمع البيانات والمراقبة عبر الإنترنت

على الرغم من استخدام مصطلحات "جمع البيانات عبر الإنترنت" و"المراقبة عبر الإنترنت (أو المراقبة الرقمية)" بشكل متبادل في كثير من الأحيان، إلا أن هناك اختلافات بينها. يُشير جمع البيانات عبر الإنترنت إلى عملية جمع المعلومات حول الأفراد وأنشطتهم عبر الإنترنت وتخزينها ومعالجتها. يمكن جمع المعلومات من خلال ملفات تعريف الارتباط على مواقع الويب، وتسجيل المستخدم، واستطلاعات الرأي عبر الإنترنت، وما إلى ذلك. في أوروبا على وجه الخصوص، يتطلب هذا النوع من الجمع علم المستخدم وموافقته. وبالنسبة لجميع الأنشطة الحكومية، يجب أن يكون جمع البيانات الشخصية عبر الإنترنت منظماً، وأن يكون لديه غرض شرعي محدد في القانون، وأن يكون متناسباً وضرورياً لتحقيق هذا الغرض الشرعي، ويجب استخدامه لهذا الغرض<sup>25</sup> إلا أن جمع تلك البيانات ومعالجتها لا تتطلب بالضرورة تحويلاً مسبقاً مستقلاً ورقابة صارمة.

على سبيل المثال، سيُمكن لضابط الشرطة الذي أوقف مركبة بسبب مخالفة مرورية، أن يُدقق في رخصة السائق ويقارنها بقاعدة بيانات السائقين الذين تم تعليق رخص قيادتهم أو يُدقق لوحة الترخيص مقارنة بقاعدة بيانات المركبات المسروقة دون الحاجة إلى تحويل قضائي مسبق. علاوة على ذلك، يدرك السائقون المرخصون أن بياناتهم الشخصية تُجمع وتُخزن وتُعالج من قبل الوكالات الحكومية لأغراض السلامة المرورية.

ومع ذلك، لا تمكن معالجة فئات معينة من البيانات، مثل البيانات الجينية، والبيانات الشخصية المتعلقة بالجرائم، والإجراءات الجنائية والإدانات، والإجراءات الأمنية المتصلة، والبيانات البيومترية التي تعرف شخصاً بعينه، والبيانات الشخصية بسبب المعلومات التي تكشفها حول الأصل العرقي أو الإثني، أو الآراء السياسية، أو العضوية في نقابة عمالية، أو المعتقدات الدينية أو غيرها، أو الصحة أو الحياة الجنسية، إلا بموجب أمر قانوني وبوجود إجراءات وقائية مناسبة لمواجهة المخاطر المحتملة للتمييز أو التأثير القانوني السلبي الذي يؤثر بشكل كبير على أصحاب البيانات. ويمكن أن تكون الإجراءات الوقائية ذات طابع تقني، على سبيل المثال، إجراءات أمنية إضافية، وتكون ذات طابع تنظيمي أيضاً. ويجب تعديل الإجراءات الوقائية لكل عملية معالجة للبيانات بما يأخذ خصوصياتها في الاعتبار. ويُوصى بشدة باستخدام مستويات متعددة من الحماية لتلك الفئات من البيانات (على سبيل المثال: أنظمة رئيسية منفصلة، وفترات أقصر لتخزين البيانات، إلخ). بالإضافة إلى ذلك، من الأهمية بمكان وضع إجراءات أمنية محددة لمنع الوصول غير المصرح به أو غير المرغوب فيه إلى تلك الفئات من البيانات<sup>26</sup>.

على النقيض من الجمع العادي للبيانات ومعالجتها، تشمل المراقبة عبر الإنترنت رصد أنشطة أفراد وكيانات محددة على الإنترنت من قبل قوات الأمن، وتتم عادةً دون علمهم أو موافقتهم. ويستدعي غياب العلم والموافقة إشرافاً أكثر صرامة إن لم يستدع الشفافية الكاملة في جميع الأوقات.

ونظراً لأن جميع أشكال المراقبة – البدنية والإلكترونية والرقمية – تثير عموماً قضايا أخطر حول الخصوصية، فإنها تتطلب إشرافاً أكثر حزمًا من الأشكال الأخرى لجمع البيانات الشخصية. ويركز هذا الدليل بشكل أساسي على جمع البيانات الشخصية في سياق عمليات المراقبة.

25 انظر على سبيل المثال، مجلس أوروبا، الدليل العملي لاستخدام البيانات الشخصية في قطاع الشرطة، القسمان 2 و3. متوفر على الرابط: <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

26 المرجع نفسه، القسم 4. متوفر على الرابط: <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

## 4 - 3 البيانات الوصفية

تعرف البيانات الوصفية عموماً على أنها "مجموعة من البيانات التي تصف بيانات أخرى وتقدم معلومات عنها". كان يُعتقد سابقاً أن جمع البيانات الوصفية المتعلقة بالاتصالات أقل خطورة من جمع محتوى الاتصالات. فقد اعتبرت المحكمة الأوروبية لحقوق الإنسان، على سبيل المثال، أن بيانات الاتصالات تشكل "عنصراً أساسياً" للاتصال الخاص وبالتالي تتمتع بدرجة من الحماية بموجب المادة 8 وإن كانت أقل من تلك الممنوحة لمحتوى الاتصال<sup>27</sup>. مع ذلك، ونظراً للتطورات في التكنولوجيا، يمكن أن تكشف البيانات الوصفية، بما في ذلك تحديد مالك عنوان بروتوكول الإنترنت IP، وبيانات المشترك، ومعرف الهاتف المحمول، أو عنوان IP للبريد الإلكتروني، أو معرف المشترك للهاتف المحمول (IMSE)، وعناوين البريد الإلكتروني، عن معلومات حساسة للغاية في بيئة يترك فيها الأفراد آثارهم الإلكترونية خلفهم في المحتوى الرقمي الخاص بهم. وبالتالي، قد تكون البيانات الوصفية بديلاً عن المحتوى المحمي للاتصالات، ونتيجة لذلك، قد يكون جمع مثل هذه البيانات تدخلية للغاية<sup>28</sup>. في الواقع، خلصت محكمة أوروبية منفصلة، هي محكمة العدل للاتحاد الأوروبي، أن "البيانات، في مجملها، قد تؤدي إلى استنتاجات دقيقة جداً بشأن الحياة الخاصة للأشخاص الذين يتم الاحتفاظ ببياناتهم، مثل العادات اليومية، وأماكن الإقامة الدائمة أو المؤقتة، والتحركات اليومية أو سواها، والأنشطة التي يقومون بها، والعلاقات الاجتماعية لهؤلاء الأشخاص، والبيئات الاجتماعية التي يترددون عليها. وتوفر تلك البيانات خصوصاً وسيلة لبناء ملف شخصي للأفراد المعنيين، وهي معلومات لا تقل حساسية، بالنظر إلى حق الخصوصية، عن المحتوى الفعلي للاتصالات"<sup>29</sup>. ونتيجة لذلك، أصبح التمييز بين تحديد البيانات الشخصية والبيانات الوصفية التي تبدو مجهولة الهوية ظاهرياً أمراً مصطنعاً وصعب التبرير بشكل متزايد.

## 4 - 4 المبادئ التوجيهية

يُمكن للدول، بموجب القانون الدولي لحقوق الإنسان، أن تنتقص من<sup>30</sup> بعض الحقوق وتفرض قيوداً على ممارستها. إلا أن بعض الحقوق تعتبر مطلقة ولا يمكن الانتقاص منها أو تقييدها<sup>31</sup>. ولأغراض هذا الدليل، سيتم التركيز فيما يلي على شروط تقييد الحقوق المشروطة. يجب أن يكون أي تدخل في حقوق الإنسان المشروطة، مثل حق الخصوصية وحرية التعبير والتجمع، منصوصاً عليه في القانون وضرورياً لحماية هدف شرعي (بما في ذلك الأمن القومي، والنظام العام، والسلامة العامة، أو حقوق الآخرين وحررياتهم). يجب أيضاً أن يكون أي إجراء محكوماً بمبادئ الضرورة والتناسب. وبناءً على ذلك، يجب أن تحترم القيود على حقوق الإنسان حظر التمييز دائماً<sup>32</sup>.

27 انظر المحكمة الأوروبية لحقوق الإنسان، منظمة بيغ بروذر ووتش وآخر ضد المملكة المتحدة، ومالون ضد المملكة المتحدة، (1985)، الفقرة 8.

28 موجز المادة 19 من أصدقاء المحكمة، مؤسسة الحدود الإلكترونية، مؤسسة كاريزما، ومنظمة الخصوصية الدولية في محكمة البلدان الأمريكية لحقوق الإنسان في قضية أعضاء مجموعة المحامين خوسيه ألفر ريس تريبو ضد كولومبيا، الصفحة 10. <https://www.law.berkeley.edu/wp-content/uploads/2022/05/Amicus-Brief-CCAJAR-v.-Colombia.pdf>.

29 الأحكام في القضية C-623/17، الخصوصية الدولية، وفي القضايا المشتركة C-511/18، (تربيع الشبكة) La Quadrature du Net وآخرون، C-512/18، شبكة البيانات الفرنسية وآخرون، وC-520/18، نظام النقابات الناطقة بالفرنسية والألمانية وآخرون، الفقرة 117.

30 عند مواجهة حالة طوارئ عامة "تهدد حياة الأمة"، يمكن للدول تعديل بعض التزاماتها في مجال حقوق الإنسان مؤقتاً، رهناً بمجموعة من الشروط. لمزيد من التفاصيل حول الاستثناءات: اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 29 "حالات الطوارئ" (المادة 4)، CCPR/C/21/Rev.1/Add.11.

31 وتشمل هذه الحقوق حظر التعذيب والمعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة، وحظر الاسترقاق والاستعباد، فضلاً عن مبدأ الشرعية الذي يقضي بعدم وجود عقوبة دون قانون. وتعني الطبيعة المطلقة لهذه الحقوق أنه لا يجوز تقييدها من خلال الموازنة بين المتع بها والسعي لتحقيق هدف مشروع، بما في ذلك في حالة النزاع المسلح، أو أي حالة من حالات الطوارئ العامة.

32 راجع، على سبيل المثال، مبادئ سيراكوزا المتعلقة بتقييد وإلغاء العهد الدولي الخاص بالحقوق المدنية والسياسية (E/CN.4/1985/4، الملحق): اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 37، المادة 21 حول الحق في التجمع السلمي، CCPR/C/GC/37، الفقرات 36، و 46؛ اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 34، المادة 19: حريات الرأي والتعبير، CCPR/C/GC/34، الفقرة 32.

## 4 - 4 - 1 المنصوص عليها في القانون

يجب أن يكون هناك أساساً في القانون المحلي لأية إجراءات لمكافحة الإرهاب التي قد تقيد من حقوق الإنسان. ويجب أن يكون هذا الأساس القانوني الداخلي متوقفاً بما فيه الكفاية، ومتاحاً، ويوفر ضمانات كافية ضد إساءة الاستخدام كالمراجعة والإشراف المستقلين، ويجب أن يوفر تعويضاً فعالاً في حالة انتهاك حقوق الإنسان. ويعني كون القانون متوقفاً أن يصاغ بدقة كافية لتمكين الفرد من تنظيم سلوكه بناءً عليه<sup>33</sup> وتمكين السلطات المختصة من التحقق من إمكانية تقييد الحقوق وتحديد نطاق أي تحفظ يطالها بالإضافة إلى طريقة تنفيذه<sup>34</sup>. ويجب أن يكون القانون متاحاً كفاية بحيث يتمكن الأفراد من الاطلاع على محتواه<sup>35</sup>. كما يجب أن يُتخذ قرار السماح بالتدخل في حق الخصوصية، من خلال إصدار أمر قضائي على سبيل المثال، من قبل سلطة مستقلة معينة بموجب القانون حصراً، وعلى أساس كل حالة على انفراد<sup>36</sup>. أما القواعد أو الإرشادات السرية، أو تفسيرات القواعد فلا تمتلك صفة "القانون"<sup>37</sup>. وأخيراً، يجب أن تُسن القوانين بشكل ديمقراطي<sup>38</sup>.

## 4 - 4 - 2 الهدف المشروع

يجب أن تكون القيود على حقوق الإنسان ضرورية لحماية أهداف مشروعة، مثل الأمن الوطني، أو النظام العام/الأمن العام، أو الصحة أو الأخلاق العامة، أو حقوق الآخرين وحررياتهم<sup>39</sup>. ويمكن أن تشكل "مصالح الأمن الوطني" سبباً لفرض القيود "إذا كانت هذه القيود ضرورية للحفاظ على قدرة الدولة على حماية وجود الأمة، أو سلامة أراضيها أو استقلالها السياسي ضد تهديد أو استخدام فعلي للقوة"<sup>40</sup>.

إلا أن الدول قد لجأت في بعض الأحيان إلى أولويات الأمن الوطني على نحو خاطئ، وتحديدًا في مكافحة الإرهاب، كذريعة لتبرير تداخلات غامضة وتعسفية في حقوق الإنسان. "يثير استخدام مفهوم غامض للأمن الوطني لتبرير قيود تدخلية على التمتع بحقوق الإنسان قلقاً كبيراً. حيث يعرّف هذا المفهوم بشكل واسع وبالتالي يصبح عرضة للاستغلال من قبل الدولة كوسيلة لتبرير أفعال تستهدف فئات ضعيفة مثل المدافعين عن حقوق الإنسان أو الصحفيين أو النشطاء السلميين. كما أنه يعمل على تبرير التكتّم المفرط غالباً حول التحقيقات أو أنشطة إنفاذ القانون، مما يقوض مبادئ الشفافية والمساءلة"<sup>41</sup>.

33 انظر على سبيل المثال اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 34. المادة 19: حريات الرأي والتعبير، CCPR/C/GC/34، الفقرة 25 وما يليها؛ المحكمة الأوروبية لحقوق الإنسان، صنداي تايمز ضد المملكة المتحدة (رقم 1)، الطلب رقم 74/6538، 26 نيسان/أبريل 1979، § 49.

34 انظر على سبيل المثال اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 34. المادة 19: حريات الرأي والتعبير، CCPR/C/GC/34، الفقرة 25؛ المحكمة الأوروبية لحقوق الإنسان، مالون ضد المملكة المتحدة، الطلب رقم 79/8691، 2 آب/أغسطس 1984، §§ 66-68.

35 انظر على سبيل المثال اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 34. المادة 19: حريات الرأي والتعبير، CCPR/C/GC/34، الفقرة 25؛ المحكمة الأوروبية لحقوق الإنسان، راديو غروبيرا أي جي وآخرون ضد سويسرا، الطلب رقم 84/10890، السلسلة أ رقم 173، 28 آذار/مارس 1990، §§ 65-68.

36 اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 16، الفقرة 8، موفر على الرابط: <https://www.refworld.org/docid/453883f922.html>.

37 تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/27/37، الفقرة 29. انظر أيضاً، المحكمة الأوروبية لحقوق الإنسان، مالون ضد المملكة المتحدة، (1985)، ECHR 14 7، الفقرتان 67 و68، متوفر على الرابط: [https://www.stradalex.com/nl/sl\\_src\\_publ\\_jur\\_int/](https://www.stradalex.com/nl/sl_src_publ_jur_int/)؛ اللجنة الأفريقية لحقوق الإنسان والشعوب، المبادئ والتوجيهات بشأن حقوق الإنسان والشعوب أثناء مكافحة الإرهاب في أفريقيا، الجزء 11، أ: يجب أن يكون الإطار القانوني المتعلق بأي تدخل في الخصوصية، وكذلك إجراءاته، في متناول العامة. متوفر على الرابط: [https://www.achpr.org/document/echr\\_869179](https://www.achpr.org/document/echr_869179)؛ <https://www.achpr.org/legalinstruments/detail?id=9>.

38 انظر، المحكمة الأفريقية لحقوق الإنسان والشعوب، س ع ص ضد جمهورية بنين، الحكم الصادر في 27 تشرين الثاني/نوفمبر 2022، الفقرتان 101 و102، وخلصت إلى أن القانون المطعون فيه تم اعتماده بشكل غير قانوني بإجراءات موجزة، وأن الفشل الإضافي في نشر القانون يشكل انتهاكاً للحق في الحصول على المعلومات، الفقرتان 111-121. متوفر على الرابط: <https://africanlii.org/afu/judgment/african-court/2020/3/>.

39 انظر على سبيل المثال، المحكمة الأوروبية لحقوق الإنسان، المادة 8 (2)؛ لجنة البلدان الأمريكية لحقوق الإنسان، المادتان 13 (2) (ب) و30؛ اللجنة الأفريقية لحقوق الإنسان والشعوب، المادة 11. انظر أيضاً، اللجنة الأفريقية لحقوق الإنسان والشعوب، المبادئ والتوجيهات بشأن حقوق الإنسان والشعوب أثناء مكافحة الإرهاب في أفريقيا، المبدأ العام م.

40 مبادئ سيراكويوزا المتعلقة بتقييد وإلغاء العهد الدولي الخاص بالحقوق المدنية والسياسية (E/CN.4/1985/4، الملحق)، الفقرة 29؛ اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 37، المادة 21 بشأن الحق في التجمع السلمي، CCPR/C/GC/37، الفقرة 42.

41 تقرير فرانك لارو، المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، A/HRC/23/40، الفقرة 58. [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)

## 4 - 4 - 3 الضرورة والتناسب

كما أن تطبيق القيود يجب ألا يتم لتحقيق هدف مشروع فقط، إنما يجب أن تكون هذه القيود ضرورية لحماية هذا الهدف. يصل متطلب ضرورة حماية الهدف إلى مستوى يتجاوز كونه "مجرد أمر منطقي أو ملائم" مع عتبة تفوق كونه مجرد أمر منطقي. من حيث المبدأ، القياس ينتهك اختبار الضرورة إذا كان بالإمكان تحقيق الحماية بطرق أخرى لا تقيّد الحق المعني.

يجب أن تتناسب الإجراءات المقيدة لحق مشروع مع الهدف المشروع المنشود، ويجب أن تكون ملائمة لتحقيق وظيفتها الوقائية وأن تكون الأقل تدخلاً بين غيرها من الإجراءات التي قد تحقق النتيجة المرجوة، ويجب أن تكون متناسبة مع المصلحة الواجب حمايتها<sup>42</sup>. على سبيل المثال، في قضية أمام المحكمة الأوروبية لحقوق الإنسان، قررت المحكمة أن "الاحتفاظ العشوائي والشامل" بالحمض النووي يُعتبر "تدخلاً غير متناسب" في الحياة الخاصة للأشخاص الذين تم جمع بياناتهم. وركزت المحكمة خصوصاً على حقيقة أن المواد "حفظت لأجل غير مسمى" بغض النظر عن طبيعة أو خطورة الجناية التي كان يشتبه في الشخص بارتكابها، وهو اعتبار مناسب بشكل خاص في القضية حيث تم تبرئة أحد المتهمين وتوقفت القضية ضد الثاني<sup>43</sup>.

## 4 - 4 - 4 عدم التمييز

يعد حظر التمييز في القانون الدولي لحقوق الإنسان مطلقاً ولا يمكن انتقاصه أو تقييده<sup>44</sup>. تشمل الأسس المحمية، ولا تقتصر على: الجنس، أو العرق، أو اللون، أو الأصل الإثني، أو اللغة، أو الدين، أو الآراء السياسية أو غيرها، أو الأصل الوطني أو الاجتماعي، أو أي وضع آخر.

## 4 - 5 حقوق أصحاب البيانات

يوجد عدد قليل جداً من القوانين الدولية بشأن حقوق أصحاب البيانات. يحظر قانون الاتحاد الأوروبي المعني بالتدخل التعسفي في حقوق الخصوصية وحرية التعبير، بما في ذلك الحق في البحث عن المعلومات<sup>45</sup>، وحق حرية التجمع، وحظر التمييز من بين أمور أخرى. ويتطلب قانون الاتحاد الأوروبي في جوهره، وكحد أدنى، أن يكون لدى الأشخاص المتأثرين بجمع البيانات ومعالجتها عبر الإنترنت حق العلم بأن البيانات الشخصية تم الاحتفاظ بها ومعالجتها، والحق في الوصول إلى البيانات المخزنة، وتصحيح البيانات غير الدقيقة أو القديمة، وحذف البيانات المحفوظة بشكل غير مشروع أو غير لازم أو تنقيحها. بالإضافة إلى حقهم في الاعتراض على

42 انظر على سبيل المثال، اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 31، الفقرة 6. اللجنة الأفريقية لحقوق الإنسان والشعوب، المبادئ والتوجيهات بشأن حقوق الإنسان والشعوب أثناء مكافحة الإرهاب في أفريقيا، المبدأ العام م. <https://www.achpr.org/legalinstruments/detail?id=9>.

43 المحكمة الأوروبية لحقوق الإنسان، س وماربر ضد المملكة المتحدة (2009) 48EHRH 50 في الفقرة 118. في هذه القضية، تمت تبرئة أحد المتهمين وتوقفت القضية ضد الثاني. اعترفت حكومة المملكة المتحدة نفسها بأن الاحتفاظ ببيانات الحمض النووي "لم يكن مبرراً بأي درجة من الشك في تورط المدعين في جريمة أو نزوعهم إلى الجريمة كما لم يكن موجهاً للاحتفاظ بالسجلات فيما يتعلق بالجرائم المزعومة التي تم التحقيق فيها في الماضي. وبشأن مبدأ التناسب أيضاً، انظر: محكمة البلدان الأمريكية لحقوق الإنسان، روشي أتانيا ضد نيكاراغوا والمزايا والتعويضات. الحكم الصادر في 3 حزيران/يونيه 2020. السلسلة ج رقم 403، الفقرة 53.

44 انظر، على سبيل المثال، الإعلان العالمي لحقوق الإنسان (المادتان 1 و2) والعهد الدولي الخاص بالحقوق المدنية والسياسية (المادة 26)، فضلاً عن اتفاقية القضاء على التمييز العنصري. فقد ذكرت محكمة البلدان الأمريكية لحقوق الإنسان، على سبيل المثال، أن "مبدأ المساواة أمام القانون، والحماية المتساوية أمام القانون، وعدم التمييز تنتمي إلى القواعد الأمرة، لأن الهيكل القانوني للنظام العام الوطني والدولي برمته يقوم عليه وهو مبدأ يتخلل كل قانون". محكمة البلدان الأمريكية لحقوق الإنسان، الرأي الاستشاري OC-18/03 بشأن الوضع القانوني للمهاجرين غير الشرعيين وحقوقهم، 17 أيلول/سبتمبر 2003، الفقرة 101. اللجنة الأفريقية لحقوق الإنسان والشعوب، المبادئ التوجيهية بشأن حقوق الإنسان والشعوب أثناء مكافحة الإرهاب في أفريقيا، دعا المبدأ العام (ز) لجنة القضاء على التمييز العنصري الدول إلى ضمان ألا تنطوي أي إجراءات يتم اتخاذها في مكافحة الإرهاب على تمييز، في الغرض أو التأثير، على أساس العرق أو اللون أو الأصل أو القومي أو الإثني، وألا يتعرض غير المواطنين للتنميط أو القوالب النمطية العنصرية أو الإثنية.

45 حرية المعلومات جزء لا يتجزأ من الحق الأساسي في حرية التعبير. انظر على سبيل المثال، <https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-of-information/#:~:text=Freedom%20of%20information%20is%20an,right%20of%20freedom%20of%20expression>.

معالجة البيانات الشخصية، ما لم تثبت الدولة أو الكيان المعالج أسباباً مشروعة لجمع تلك البيانات ومعالجتها، وحققهم في الحصول على تعويض عند انتهاك حقوقهم<sup>46</sup>.

ومع ذلك، قد توجد قيود على هذه القواعد العامة في سياق أنشطة إنفاذ القانون وعملياته عندما ينص القانون على هذه القيود، وتحترم جوهر الحقوق والحريات الأساسية وتشكل إجراءً ضرورياً ومتناسباً في مجتمع ديمقراطي، يتضمن ذلك، ولا يقتصر على: حماية الأمن القومي أو منع الجرائم الجنائية والتحقيق فيها ومحاكمتها<sup>47</sup>. على سبيل المثال: عند التحقيق مع مشتبه فيه عالي الخطورة ومراقبته، يمكن تبرير معالجة البيانات والاحتفاظ بها لفترة طويلة، دون إبلاغ الفرد الذي يخضع للمراقبة إذا كان تنبيه الهدف قد يؤدي إلى التشويش على التحقيق الجاري أو المزمع. ولكن بمجرد تحقق الغرض من المراقبة الخفية، وعدم وجود أي قيود أخرى نافذة، يجب إعلام الهدف بأنه تعرض لهذا التدبير. وقد تكون هناك ظروف أخرى تبرر فيها القيود على الحق في الوصول إلى المعلومات المتعلقة بالبيانات المعالجة، على سبيل المثال، إذا أدى تزويد صاحب البيانات بالمعلومات إلى تعريض سلامة شاهد أو مخبر للخطر. أو إذا أشارت معلومات استخباراتية محددة إلى تنفيذ عمليات غسيل أموال لتمويل عمليات إرهابية، فقد يتم الاحتفاظ بالبيانات التي جمعت عن الأفراد لفترة أطول من اللازم بخلافه لأغراض التحقيق الفردي بعد مصادقة هيئة رقابة خارجية. ولكن لا يجب اللجوء إلى الاحتفاظ بالمعلومات حول معالجة البيانات من قبل الشرطة إلا فيما ندر بحيث يمكن تبريرها بوضوح<sup>48</sup>.

46 قام مجلس أوروبا بتحديث الاتفاقية رقم 108 لحماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية. انظر أيضاً المادة 21 من اللائحة العامة لحماية البيانات للاتحاد الأوروبي والمادة 18 (1) من اتفاقية مالايو بشأن الأمن السيبراني وحماية البيانات الشخصية.

47 المرجع نفسه، المادة 11.

48 مجلس أوروبا، دليل عملي حول استخدام البيانات الشخصية في قطاع الشرطة، الأقسام 5,7. متوفر على الرابط: <https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>.

## [خامسا]

# الشفافية وآليات الرقابة

## 5 - 1 ملحة عامة

على الرغم من ندرة الأدوات الدولية أو الإقليمية التي تحدد نوعية آليات الرقابة المطلوبة من الدول الأعضاء، إن وجدت، فإن الالتزامات الإجرائية تنبع من الالتزامات الموضوعية. وقد أكدت المحكمة الأوروبية لحقوق الإنسان أنه من أجل ضمان الحقوق والحريات، لا تلزم الاتفاقية السلطات العليا في الدول الموقعة أنفسها فحسب باحترام الحقوق المعنية، وإنما تفرض عليها أن تمنع أو تعالج أي انتهاك على المستويات الأدنى.<sup>49</sup>

تتطلب الممارسات المثلى، في حدها الأدنى، وجود قواعد داخلية تتعلق بجمع البيانات ومعالجتها؛ والمصادقة على جمع البيانات شديد التدخل، مثل عمليات المراقبة، من قبل هيئة مستقلة، عادة ما تكون سلطة قضائية؛ ووجود هيئات رقابية مدنية فعالة أثناء عمليات إنفاذ القانون وبعدها؛ وتوفير المعلومات ونشرها حول جمع بيانات الأفراد ومعالجتها من قبل الحكومة؛ ووجود هيئات فعالة ومستقلة قادرة على توفير الحلول لانتهاك حقوق الأهداف، بما في ذلك الهيئات القضائية.

لكي يكون نظام الرقابة فعالاً، يُوصى بوجود ست ركائز متكاملة من الرقابة والضبط على الأقل؛ وتشمل:

- الرقابة الداخلية ضمن وكالات إنفاذ القانون؛
- الضبط التنفيذي (ضبط السياسات، والضبط المالي، والرقابة الأفقية من قبل الوكالات الحكومية)؛
- الرقابة البرلمانية (أعضاء البرلمان، ولجان التحقيق البرلمانية)؛
- المراجعة القضائية؛
- الرقابة من خلال هيئات مستقلة مثل المؤسسات الوطنية لحقوق الإنسان، وأمناء المظالم، وغيرهم؛
- رقابة المجتمع المدني.<sup>50</sup>

## 5 - 2 هيئات الرقابة الفعالة

لكي تكون هيئات الرقابة فعالة، يجب أن تكون قادرة على الشروع في تحقيقات مستقلة وإجرائها، وأن تمتلك موارد كافية من حيث الميزانية والخبرات والمواد، وأن تحظى بإمكانية الوصول الكامل دون عوائق إلى المعلومات والمنشآت والمسؤولين<sup>51</sup>. على سبيل المثال،

49 أسانديزي ضد جورجيا (71503/01) – الحكم الصادر في 8 نيسان/أبريل 2004.

50 مجلس أوروبا، آليات رقابة الشرطة في الدول الأعضاء في مجلس أوروبا، القسم 3، الصفحة 67، متوفر على الرابط: <https://rm.coe.int/police-oversight-mechanisms-in-the-coe-member-states/16807175dd>.

51 تقرير مارتن شاينين، المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، مجموعة الممارسات الجيدة بشأن الأطر والإجراءات القانونية والمؤسسية التي تضمن احترام وكالات الاستخبارات لحقوق الإنسان في سياق مكافحة الإرهاب، بما في ذلك احترامها الرقابة، A/HRC/14/46، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>.

يجب أن تملك هيئات الرقابة إمكانية الوصول إلى كافة المعلومات المعنية، بغض النظر عن مستوياتها التصنيفية، والتي تراها متصلة بتحقيق مهامها. وينبغي أن تحفظ إمكانية وصول هيئات الرقابة إلى المعلومات في نص القانون الذي يحدد مهامها وسلطاتها. كما يجب منع أي محاولات لتقييد وصول هيئات الرقابة إلى المعلومات السرية وأن تخضع للعقوبة عند الضرورة. مع ذلك، قد يكون من الضروري تنقيح التقارير العامة بشأن المعلومات التي تحدد الأهداف المحتملين والشهود والأساليب الفردية.

تتمتع الأجهزة الأمنية بقدرات متطورة بشكل متزايد لجمع المعلومات ومشاركتها واستقبالها وتستخدم أنظمة متزايدة التعقيد للقيام بذلك. بناء عليه، قد تحتاج هيئات الرقابة إلى خبرات تقنية مستقلة لفهم طريقة عمل الأنظمة المختلفة.

## 5 - 2 - 1 هيئات الرقابة المستقلة

آليات الرقابة المستقلة تتمتع باستقلالية عن الأهداف السياسية أو الاقتصادية أو العسكرية أو غيرها. ولديها (1) استقلالية رسمية (بحكم القانون) تتطلب بقاءها خارج التسلسل البيروقراطي والهرمي في الوزارات أو الوكالات الحكومية الأخرى؛ و(2) استقلالية فعلية (بحكم الواقع) تتعلق بحق الوكالة في تقرير المصير حول إجراء التحقيقات وضمان الجبر أو التعويض أو التوصية به<sup>52</sup>.

## 5 - 3 الموافقة المستقلة المسبقة لعمليات المراقبة والتحقيق الخاصة

لقد أقرت اللجنة المعنية بحقوق الإنسان بأن التصريح لأي تدخل في حق الخصوصية، بما في ذلك إجراءات المراقبة، يجب ألا يصدر إلا عن السلطة المعينة بموجب القانون، وعلى أساس كل حالة على حدة<sup>53</sup>. وأشارت المحكمة الأوروبية لحقوق الإنسان إلى أن الجهة المفوضة لا يجب بالضرورة أن تكون هيئة قضائية، إلا أن تلك الهيئة غير القضائية يجب أن تتمتع باستقلال كاف عن السلطة التنفيذية. في الوقت ذاته، بينت المحكمة أن التدخل من قبل السلطات في حقوق الأفراد يجب أن يخضع لتحكم فعال، يجب ضمانه عادةً بالقضاء، كملأه أخيراً على الأقل، حيث يوفر التحكم القضائي أفضل ضمانات للاستقلالية والتجرد والإجراء السليم. كما اعتبرت المحكمة أيضاً أنه على الرغم من أن التصريح المسبق ليس مطلباً مطلقاً في حد ذاته، فإن المراجعة القضائية بأثر رجعي قد لا تكون كافية في بعض الظروف لموازنة أوجه القصور في التصريح، وبالتالي فإن التصريح القضائي المسبق ضروري<sup>54</sup>. وينطبق هذا المبدأ على كل من المراقبة الموجهة وغير الموجهة. كما يجب أن يبنى التصريح على الحقائق. على سبيل المثال، أعربت محكمة البلدان الأمريكية لحقوق الإنسان عن قلقها إزاء منح محكمة محلية تصريحاً بالمراقبة على الرغم من افتقار الطلب لأية أسباب أو أسس تبرره. كما لاحظت أن الأشخاص الذين يسعون للحصول على إذن المراقبة لم يسيروا إلى عدم توفر وسائل أقل تدخلاً للحصول على المعلومات المطلوبة<sup>55</sup>.

يجب الحصول على موافقة مسبقة على عمليات إنفاذ القانون ذات الصلة التداخلية من هيئة مستقلة قبل الانخراط في أي من الأنشطة التالية إما بشكل مباشر أو من خلال/ بالتعاون مع كيانات القطاع الخاص:

- القيام بإجراءات المراقبة الموجهة، متضمنة جمع بيانات الاتصالات والوصول إليها (بما في ذلك عند احتفاظ القطاع الخاص بها)؛
- القيام بإجراءات المراقبة الشاملة غير الموجهة بغض النظر عن الأساليب أو التكنولوجيا المستخدمة أو نوع الاتصالات المستهدفة؛

52 انظر، على سبيل المثال، قسم دليل النزاهة العامة لمنظمة التعاون الاقتصادي والتنمية 12.2.3، <https://www.oecd-ilibrary.org/sites/7715f0e0-en/>، [index.html?itemId=/content/component/7715f0e0-en](https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en)

53 التعليق العام رقم 16، الفقرة 8.

54 زاو وفيسي ضد هنجاريد، الفقرة 77.

55 ك (2009)، الفقرات 92، 134، 135، 140. كما رأيت المحكمة الأوروبية لحقوق الإنسان أنه "عندما يؤيد القاضي فقط تصرفات الأجهزة الأمنية دون التحقق بشكل حقيقي من الوقائع أو توفير الرقابة الكافية"، فإن ذلك يشكل انتهاكاً للمادة 8 من الاتفاقية. انظر قضية زولتان فارجا ضد سلوفاكيا، الفقرات 155-160.

- استخدام المحددات أو الكلمات المفتاحية لاستخراج البيانات من المعلومات المجموعة عن طريق المراقبة الشاملة، خاصةً عندما تكون هذه المحددات متعلقة بأشخاص يمكن تعريفهم؛
- جمع الاتصالات/البيانات الوصفية مباشرةً أو الوصول إليها من خلال طلبات تُقدّم إلى أطراف ثالثة، بما في ذلك الشركات الخاصة؛
- القيام بالاستغلال في شبكات الحاسوب، وهي أحد أشكال القرصنة<sup>56</sup>.

قد تناولت المحكمة الأوروبية لحقوق الإنسان عمليات المراقبة في عدد من القضايا والمبادئ القائمة قابلة للتطبيق على جميع أشكال المراقبة. يجب أن تتضمن التصاريح المستقلة للمراقبة:

- تفاصيل الأفراد الذين ستتم مراقبة اتصالاتهم؛
- طبيعة الجرائم التي تبرر التدخل؛
- مدة المراقبة؛
- الإجراءات المتبعة لإعداد التقارير الموجزة حول الاتصالات المعترضة؛
- الاحتياطات الواجب اتخاذها من أجل الحفاظ على سلامة وأمن المواد المعترضة؛
- الظروف التي يجب فيها محو المعلومات المعترضة أو إتلافها، بما في ذلك الأجل المحدد، على سبيل المثال، بعد إخلاء سبيل المتهم أو براءته<sup>57</sup>.

يجب أن يضمن الجهاز المستقل والفعال الذي يمنح التصريح بإجراءات المراقبة أن يكون هناك دليل واضح على تهديد كاف وأن تكون المراقبة المقترحة موجهة وضرورية بشكل صارم ومتناسبة وأن يصرح (أو يرفض) إجراءات المراقبة مسبقاً<sup>58</sup>. تنطبق المبادئ ذاتها عندما تسعى أجهزة إنفاذ القانون للحصول على البيانات الشخصية من القطاع الخاص.

### 5 - 3 - 1 الرقابة أثناء العمليات والمراجعة اللاحقة للأنشطة والعمليات

أشارت اللجنة المعنية بحقوق الإنسان إلى أن برامج المراقبة والاعتراض والقرصنة لا يمكن أن تتوافق مع حقوق الإنسان إلا في وجود آليات رقابة قوية ومستقلة<sup>59</sup>.

تشكل آليات التحكم الداخلية ضمن جهاز الشرطة الدرجة الأولى من التحكم في أي نظام لمساءلة الشرطة. حيث تساعد الضوابط الفعالة في منع سوء التصرف ومعالجته. وتتألف هذه الآليات من ثلاث مكونات رئيسية هي:

- معايير المهنية والنزاهة؛
- الإشراف والمراقبة المستمرة؛
- الإبلاغ الداخلي والإجراءات التأديبية.

56 مجلس أوروبا، الرقابة الديمقراطية والفعالة على أجهزة الأمن القومي، الصفحة 12، متوفر على الرابط: <https://book.coe.int/en/commissioner-for-human-rights/6682-pdf-democratic-and-effective-oversight-of-national-security-services.html>

57 منظمة الأمن والتعاون في أوروبا/مكتب المؤسسات الديمقراطية وحقوق الإنسان، حقوق الإنسان في التحقيقات المتعلقة بمكافحة الإرهاب: دليل عملي لموظفي إنفاذ القانون، الحاشية 48 التي تشير إلى مكافحة الإرهاب وحماية حقوق الإنسان: دليل، الصفحة 205، الحاشية السفلية 687 نقلاً عن المحكمة الأوروبية لحقوق الإنسان، هوفنغ ضد فرنسا، القضية رقم 220/164/1989/4، 27 آذار/مارس 1990، الفقرات 32-33؛ المحكمة الأوروبية لحقوق الإنسان، كروسلين ضد فرنسا، الطلب رقم 85/11801، 24 نيسان/أبريل 1990، الفقرة 35؛ المحكمة الأوروبية لحقوق الإنسان، غريوتر ضد هولندا، الطلب رقم 98/40045، 19 آذار/مارس 2002.

58 تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/39/29، الفقرة 39، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>

59 الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، مجموعة الممارسات الجيدة بشأن الأطر والإجراءات القانونية والمؤسسية التي تضمن احترام وكالات الاستخبارات لحقوق الإنسان في سياق مكافحة الإرهاب، بما في ذلك الرقابة عليهم، A/HRC/14/46، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

لذلك، من الإلزامي أن تطوّر أجهزة الشرطة معايير مهنية شاملة (قواعد السلوك، وأخلاقيات العمل)، توفر توجيهات واضحة حول الممارسة العملية لواجبات الشرطة وصلاحياتها.

تشكل السلطة القضائية عنصراً أساسياً في نظام المساءلة الخاص بالشرطة. حيث يجب أن تحصل أنشطة المراقبة أو جمع البيانات السرية على تصريح من جهة قضائية أو هيئة تمثيل قضائي، أو من خلال آلية مستقلة مماثلة، قبل البدء بتلك الأنشطة، قدر الإمكان. يراقب قضاة التحقيق، في الأنظمة القانونية المدنية، أنشطة إنفاذ القانون أثناء إجراءاتها. وفي جميع الأنظمة، يجب أن تُكلف السلطة القضائية بالنظر في الادعاءات بشأن سوء التصرف في إنفاذ القانون وفرض العقوبات والجزاءات.

أحد أهم الأدوار الأساسية للبرلمانات في جميع أنحاء العالم هو صياغة القوانين وتعديلها وسنها. بالتالي، يجب على هذه الهيئات وضع أطر قانونية واضحة ودقيقة ومتاحة وغير تمييزية بشأن برامج مراقبة إنفاذ القانون، تتماشى مع القانون الدولي، بما في ذلك المعايير والقواعد الدولية لحقوق الإنسان. بالإضافة إلى ذلك، ونظراً لأن الهيئات التشريعية مسؤولة عن متابعة صلاحيات السلطة التنفيذية، فإنها غالباً ما تنشئ لجاناً رقابية دائمة أو مؤقتة وتحقيقات لمراجعة برامج المراقبة السرية.

قامت بعض الدول الأعضاء أيضاً بإنشاء هيئات خبراء مستقلة، تتضمن على سبيل المثال لا الحصر مؤسسات حقوق الإنسان الوطنية، وأمناء المظالم، و/أو سلطات حماية البيانات المفوضة بالإشراف على برامج المراقبة. إن الشكل الدقيق لهذه الهيئات الرقابية غير محكوم بالقانون الدولي، ولكنها يجب أن تكون مستقلة وتتمتع بسلطات قوية، بما في ذلك الحصول على جميع المعلومات المتعلقة بدورات المراقبة الكاملة، وتقديم توصيات ملزمة وعامة.

يمكن للأطر الرقابية دمج مزيج من الرقابة الإدارية و/أو القضائية و/أو البرلمانية. ويجب أن تكون هيئات التصريح والرقابة منفصلة مؤسسياً، على الرغم من إمكانية منح إحدى الهيئات القضائية التصريح لعملية ما، وتوفير هيئة أخرى التعويض للضحايا.

يجب على الهيئات الرقابية المستقلة أن تقوم بالتحقيق والمراقبة الوقائية لأنشطة الذين يقومون بالمراقبة ويملكون إمكانية الوصول إلى منتجات المراقبة، وأن تجري مراجعات دورية لقدرات المراقبة والتطورات التكنولوجية. ويجب أن تلتزم الجهات المنفذة للمراقبة بتوفير جميع المعلومات اللازمة للرقابة الفعالة عند الطلب، والإبلاغ بانتظام إلى الهيئات الرقابية المعنية، ويجب إلزامها بالاحتفاظ بسجلات كافة إجراءات المراقبة المتخذة<sup>60</sup>. كما يجوز لآليات الرقابة أن تقدم توصيات بشأن الإصلاحات المؤسسية والتشريعية التي يجب أن تحظى بالاعتبار الكافي من قبل الجهات التنفيذية والتشريعية المعنية.

يجب على مؤسسات الرقابة اتخاذ كافة الإجراءات اللازمة لحماية المعلومات السرية والبيانات الشخصية التي يمكنها الوصول إليها أثناء تأدية عملها، وفرض عقوبات على انتهاك هذه المتطلبات من قبل أعضاء مؤسسات الرقابة<sup>61</sup>.

## 5 - 4 آليات الشكاوى

إن وجود آليات تمكن الأفراد من تنفيذ شرعية التدخلات المزعومة في حقوق الإنسان أمر أساسي من شأنه أن يعزز تطوير مبادئ التحريات الفعالة. وقد ساهمت مشاركة الضحايا والرقابة العامة في تنامي الوعي بمصالح أصحاب البيانات. ومن أجل ضمان ثقة الجمهور في نظام الشكاوى والحفاظ عليها، يجب معالجة المظالم بشكل كاف ومناسب وفقاً لطبيعة الشكاوى.

تتضمن الأنواع الخمسة الرئيسية لآليات شكاوى الشرطة المطبقة حول العالم: الشرطة الداخلية؛ وزارة الشرطة أو الداخلية؛ النيابة العامة؛ أمين المظالم؛ الرقابة المدنية. وليس من الغريب أن تعمل عدة آليات معا ضمن نظام قضائي واحد<sup>62</sup>.

60 تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/39/29، الفقرة 40، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>

61 تقرير مارتن شاينين، المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، مجموعة الممارسات الجيدة بشأن الأثر والإجراءات القانونية والمؤسسية التي تضمن احترام وكالات الاستخبارات لحقوق الإنسان في سياق مكافحة الإرهاب، بما في ذلك احترامها الرقابة، A/HRC/14/46، الفقرة 14، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

62 المرجع نفسه.

إن إنشاء هيئة رقابة مدنية مستقلة خارجية مسؤولة عن استقبال الشكاوى ضد الشرطة والتحقيق فيها أمر أساسي لتحقيق مزيد من المساءلة والشفافية، ولعلاج عيوب التحكم والرقابة الداخليين غير الفعالين في بعض الحالات. أحد الأعراس التشريعية القياسية في الأنظمة القضائية التي تقنن نظم الشكاوى ضد الشرطة هو محاسبة مسؤولي إنفاذ القانون من خلال إجراءات جنائية تأديبية، استناداً إلى الأدلة المجموعة أثناء التحقيق في الشكاوى. يمكن للأليات ذاتها المتبعة في التحقيق في مزاعم الاستخدام المفرط للقوة من قبل الشرطة أن تستخدم أيضاً للتحقيق في مزاعم التدخل غير المشروع في الخصوصية، أو الجمع غير المشروع للبيانات الشخصية عبر الإنترنت، بالرغم من أن هذه الآلية قد تتطلب خبرة فنية إضافية. كما يوفر نظام شكاوى الشرطة الفعال الحماية الأساسية ضد تطور ثقافة الإفلات من العقاب. بالإضافة إلى ذلك، تعتبر الشكاوى مصدراً مهماً يمكن البحث فيه وتحليله لاستخلاص العبر من الأخطاء السابقة بهدف تحسين الأداء المستقبلي. وتوفر الشكاوى فرصة لتعلم الدروس على مستوى الضابط المنفرد وعلى مستوى الجهاز ككل<sup>63</sup>.

## 5 - 4 - 1 الجزاء والتعويض

تنص المادة الثانية من العهد الدولي الخاص بالحقوق المدنية والسياسية على الحق في تطبيق جزاء فعال لانتهاكات التزامات حقوق الإنسان<sup>64</sup>. وبالتالي، يجب أن يتمتع الأفراد المتأثرون بأفعال غير قانونية من جانب مسؤولي أو وكالات إنفاذ القانون بإمكانية اللجوء إلى مؤسسة قادرة على توفير الجزاء الفعال، بما في ذلك التعويض الكامل عن الضرر الذي تعرضوا له. ويمكن أن يشمل ذلك المؤسسات غير القضائية المخولة بتلقي الشكاوى والتحقيق فيها وإصدار أوامر ملزمة أو توفير جزاءات فعالة، أو المؤسسات القضائية التي يمكنها فرض إجراءات تعويضية. ولضمان التطبيق العملي لهذا الحق، يجب على الدول ضمان وصول الأفراد أيضاً إلى مؤسسة مجهزة لإصدار أوامر قانونية ملزمة بشأن التعاون، بما في ذلك المعلومات التي تم تلقيها من جهات أجنبية أو إرسالها إليها. ويجب أن تكون المؤسسات المسؤولة عن التعامل مع الشكاوى والدعاوى المطالبة بجزاء فعال والناشئة عن أنشطة أجهزة الاستخبارات، مستقلة عن وكالات إنفاذ القانون والسلطة التنفيذية. كما يجب أن تتمتع هذه المؤسسات بإمكانية الوصول الكامل دون عوائق إلى كافة المعلومات ذات الصلة، والمصادر اللازمة والخبرة لإجراء التحقيقات، والقدرة على إصدار الأوامر الملزمة<sup>65</sup>.

## 5 - 4 - 2 الشفافية

تعد الشفافية أمراً حاسماً في جميع عمليات الحكومات الديمقراطية. وبالتالي، يجب أن يكون الإطار القانوني العام المتعلق بالمراقبة بجميع أشكالها، بالإضافة إلى الإجراءات المتبعة في التصريح بالمراقبة، واختيار أهداف المراقبة، واستخدام المواد المعترضة، ومشاركتها، وتخزينها، وإتلافها، متاحاً للعامة<sup>66</sup>.

ينبغي على السلطات الحكومية وهيئات الرقابة أن تشارك في نشر المعلومات حول القوانين والسياسات والممارسات القائمة في مجال المراقبة واعتراض الاتصالات وغيرها من أشكال معالجة البيانات الشخصية، حيث إن النقاش المفتوح والتدقيق الشامل ضروريان لفهم ميزات تقنيات المراقبة وقيودها<sup>67</sup>.

63 مجلس أوروبا، إصلاح الشكاوى الدولية ضد الشرطة، متوفر على الرابط: <https://rm.coe.int/16806dbbbd>.

64 المادة 2 من العهد الدولي الخاص بالحقوق المدنية والسياسية تنص على: (أ) ضرورة ضمان أن يكون لدى كل شخص تم انتهاك حقوقه أو حرياته المعترف بها في هذا العهد حق الحصول على جزاء قانوني فعال، بغض النظر عما إذا كان الانتهاك قد ارتكب من قبل أشخاص يمارسون سلطة رسمية؛ (ب) ضرورة ضمان أن يتم تقرير حق الشخص الذي يطالب بهذا الجزاء من قبل سلطات قضائية أو إدارية أو تشريعية مختصة، أو من قبل أي سلطة مختصة أخرى ينص عليها النظام القانوني للدولة، وتطوير إمكانيات التعويض القضائي؛ (ج) ضرورة ضمان أن تنفذ السلطات المختصة هذه الجزاءات عند إقرارها.

65 تقرير مارتن شاينين، المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، مجموعة الممارسات الجيدة بشأن الأطر والإجراءات القانونية والمؤسسية التي تضمن احترام وكالات الاستخبارات لحقوق الإنسان في سياق مكافحة الإرهاب، بما في ذلك احترامها الرقابة، A/HRC/14/46، الفقرة 16-17، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>.

66 المبدأ 10. هـ من مبادئ تشواني بشأن الأمن القومي والحق في الحصول على المعلومات، متوفر على الرابط: <https://www.justiceinitiative.org/publications/> Principles%20on%20National%20Security%20and%20the%20Right%20to%20and%20national%20law%20and%20practices

67 تقرير المقرر الخاص المعني بالحق في الخصوصية، A/HRC/34/60، الفقرة 38، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement>.

ويجب إخطار أولئك الذين خضعوا للمراقبة وشرح التدخل في حقهم في الخصوصية بأثر رجعي إن لم يكن الإخطار المتزامن ممكناً. يجب أن يحق للأشخاص تعديل و/أو حذف المعلومات الشخصية غير ذات الصلة، شريطة أن تكون هذه المعلومات غير دقيقة أو لم تعد ضرورية لأغراض التحقيق الحالي أو المزمع<sup>68</sup>.

كما يجب أن تكون عمليات الرقابة شفافة وعرضة للتدقيق العام المناسب، ويجب أن تكون قرارات هيئات الرقابة عرضة للاستئناف أو المراجعة المستقلة<sup>69</sup>. كما يجب أن تلتزم هيئات الرقابة بموجب القانون بنشر النسخ العامة من تقاريرها وتحقيقاتها الدورية. بالإضافة إلى ذلك، يجب ألا تعفى وكالات إنفاذ القانون وهيئات الرقابة عموماً من تشريعات حرية المعلومات. بل يجب اتخاذ القرار بعدم نشر بعض المعلومات على أساس كل حالة على حدة، مع التبرير المناسب وخضوعها لإشراف هيئة مستقلة.

## 5 - 5 البيانات المجمعة تجارياً

في حين يتطلب القانون الدولي من الوكالات الحكومية الحصول على مذكرات أو أدونات مماثلة، امتثالاً للقانون المحلي الواضح والدقيق والمتاح والشامل وغير المميز، قبل الوصول إلى البيانات الشخصية للأفراد، يزداد الأمر تعقيداً بوجود بيانات تجارية متاحة تجمع بين المعلومات العامة والخاصة. تستخدم الجهات الحكومية التي تسعى لشراء البيانات غالباً مصطلحات مثل "المصادر المفتوحة" و"المتاحة للعموم" في أوامر الشراء والعقود، مما يوحي بأنها تسعى فقط للحصول على معلومات من مثل المنشورات العامة على وسائل التواصل الاجتماعي التي يوفرها الأشخاص للعموم عن علم منهم. ومع ذلك، تستخدم أوامر الشراء والعقود الحكومية هذه المصطلحات بشكل متكرر لتشمل المعلومات التي جمعت خصيصاً لصالح وكالة معينة ليست في الواقع متاحة للعموم أو أي عميل آخر. ويقوض الاستخدام الواسع والمضلل لهذه المصطلحات المزاعم الحكومية بأن الوكالات مخولة بجمع مثل هذه المعلومات على أساس أنها متاحة عموماً للجمهور والأفراد، وبالتالي تفتقد إلى توقع معقول للخصوصية في هذه البيانات الحساسة<sup>70</sup>. ويتوجب في الحد الأدنى، عند شراء الجهات الحكومية بيانات تشمل، على سبيل المثال، معلومات مالية أو طبية يتوقع الشخص منطقياً خصوصيتها، أن يتم شراء تلك البيانات بما يتوافق بدقة مع المبادئ المحددة في هذا التقرير. وبالرغم من كونها تقع خارج نطاق هذا الوثيقة، فإن المبادئ التوجيهية للأمم المتحدة بشأن الأعمال التجارية وحقوق الإنسان توضح التزامات الدول عند التعاقد مع المؤسسات التجارية، فضلاً عن مسؤولية هذه المؤسسات في احترام حقوق الإنسان ومنع ومعالجة كافة التأثيرات السلبية على حقوق الإنسان والمرتبطة بشكل مباشر بعملياتها أو منتجاتها أو خدماتها<sup>71</sup>.

68 تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/39/29، متوفر على الرابط: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>

69 المرجع نفسه، الفقرة 40.

70 مركز الديمقراطية والتكنولوجيا، الثغرات القانونية والبيانات الخاصة بالدولار: كيف تشتري وكالات إنفاذ القانون والاستخبارات بياناتك من الوسطاء، <https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/>

71 المبادئ التوجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة "الحماية والاحترام والانتصاف" | المفوضية السامية لحقوق الإنسان. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework | OHCHR. انظر أيضاً، تقرير مفوضة الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، A/HRC/39/29، الفقرات 42-49.

### 6 - 1 الاعتبارات الرئيسية

- 1 - يجب على الدول الأعضاء وضع آليات رقابية داخلية ومستقلة لمراقبة أنشطة مسؤولي إنفاذ القانون فيما يتعلق بجمع البيانات عبر الإنترنت والمراقبة الرقمية. يمكن دمج مسؤولية الرقابة على جمع البيانات والمراقبة عبر الإنترنت في واجبات الآليات الرقابية الحالية. كما تسهم الرقابة المدنية في تعزيز المساءلة والشفافية.
- 2 - يجب أن تكون الآليات الرقابية الخارجية مستقلة، وأن تمتلك الموارد الكافية، وأن تحظى بوصول كامل دون عائق إلى جميع المعلومات والمباني والمسؤولين المعنيين. ويمكن أن تتضمن مزيجا من الهيئات الإدارية والتنفيذية والتشريعية والمستقلة، على الرغم من ضرورة تمتع الأخيرة بسلطات التحقيق وتوفير الجزاء الفعال.
- 3 - تزداد صعوبة تبرير التمييز بين جمع البيانات الشخصية ومعالجتها وجمع البيانات الوصفية ومعالجتها.
- 4 - كما يصعب التمييز القانوني بين جمع البيانات الشخصية من قبل الحكومة وشراء البيانات الشخصية من الكيانات التجارية.
- 5 - يجب توضيح حق الوصول إلى البيانات الشخصية، والظروف التي يمكن فيها الوصول إلى هذه البيانات، بموجب قانون أو لائحة داخلية يتصفان بالوضوح والدقة والإتاحة والشمول وعدم التمييز، ويجب توزيعه على جميع ضباط إنفاذ القانون. وتجب معالجة انتهاكات هذه القواعد من خلال الآليات التأديبية الحالية أو الجديدة.
- 6 - يجب على الحكومات، حفاظا على الشفافية، توفير المعلومات للسكان حول أنشطتها في جمع البيانات ومعالجتها. ويجب أن تكون عمليات آليات الرقابة ونتائجها متاحة للعامة قدر الإمكان.
- 7 - يجب أن تضمن الدول حق أي ضحايا لجمع البيانات والمراقبة عبر الإنترنت بصورة غير شرعية في تقديم شكوى إلى محكمة مستقلة أو مؤسسة رقابية واللجوء إلى مؤسسة يمكنها توفير الجزاء الفعال، بما في ذلك التعويض الكامل عن الضرر الذي لحق بهم.
- 8 - يشكل المجتمع المدني شريكا أساسيا في العمل على ضمان احترام حقوق الإنسان في جمع البيانات الشخصية ومعالجتها. ويتم تشجيع الدول على تهيئة بيئة تمكينية للمجتمع المدني والحفاظ عليها، بما في ذلك وضع إطار قانوني يحمي حقوق الإنسان ويعززها، بما يتوافق مع القانون الدولي لحقوق الإنسان. ويجب عليها ضمان خضوع أي عقبات رسمية تمنع رقابة المجتمع المدني على جمع الحكومة للبيانات الشخصية ومعالجتها لمراجعة قضائية مستقلة.



© مكتب الأمم المتحدة لمكافحة الإرهاب، 2023  
مكتب الأمم المتحدة لمكافحة الإرهاب  
المقر الرئيسي لمنظمة الأمم المتحدة  
نيويورك، نيويورك 10017

[www.un.org/counterterrorism/ar](http://www.un.org/counterterrorism/ar)

مكتب الأمم المتحدة  
لمكافحة الإرهاب  
مركز الأمم المتحدة لمكافحة الإرهاب



24-11099