

دليل إرشادي

# فهم الإشراف على الاستخبارات

ايدان ويلز (Aidan Wills)





دليل إرشادي

# فهم الإشراف على الاستخبارات

ايدان ويلز (Aidan Wills)

مركز جنيف  
للرقابة الديموقراطية  
على القوات المسلحة



## فهم الإشراف على الاستخبارات

### هيئة التحرير

تضم هيئة التحرير التي عملت على مجموعة الكتيبات المتعلقة بالإشراف على الاستخبارات وهم:

- هانز بورن (Hans Born)، جنيف
- يان ليه (Ian Leigh)، دورهام
- أرنولد ليتهولد (Arnold Luethold)، جنيف
- بنيامين باكلاوند (Benjamin Buckland)، جنيف

### الترجمة:

محمود السيد، الشرقية

### مركز جنيف للرقابة الديمقراطية على القوات المسلحة

يعمل مركز جنيف للرقابة الديمقراطية على القوات المسلحة على تعزيز مبدأ الحكم الرشيد وإصلاح قطاع الأمن. ويُعدّ المركز الأبحاث حول أفضل الممارسات المتبعة في هذا المجال، ويشجع على نشر المعايير المرعية على المستويين المحلي والدولي. كما يقدم المركز التوصيات السياسية والاستشارات والمساعدات في هذا المجال للعديد من الدول. ويضمّ شركاء مركز جنيف للرقابة الديمقراطية على القوات المسلحة الحكومات، والبرلمانات، ومؤسسات المجتمع المدني والمنظمات الدولية، إلى جانب المؤسسات الأمنية كالشرطة والقضاء وأجهزة المخابرات وحرس الحدود والجيوش. ويعرض الموقع الإلكتروني لمركز جنيف للرقابة الديمقراطية على القوات المسلحة المزيد من المعلومات حول هذا المركز وعمله على العنوان التالي:

[www.dcaf.ch](http://www.dcaf.ch)

### شكر وتقدير

يود الكاتب أن يعرب عن امتنانه لأعضاء هيئة التحرير على تعليقاتهم القيّمة والوقت الذي بذلوه لمراجعة هذا الدليل.

كما يتقدم مركز جنيف للرقابة الديمقراطية على القوات المسلحة بالشكر إلى «انتصار أبو خلف» للمساعدة في التحرير.

### الناشر

© مركز جنيف للرقابة الديمقراطية على القوات المسلحة، 2010، جميع حقوق الطبع والنشر محفوظة

صورة الغلاف ©: رويترز، كريس واتي، ٢٠٠٧

ISBN: 978-92-9222-131-7

# المحتويات

٩	مقدمة الرزمة
١١	فهم الاشراف على الاستخبارات
١١	ما هو الهدف من هذا الدليل؟
١١	ما الذي يحتويه هذا الدليل؟
١١	من المستهدف بهذا الدليل؟
١١	ما هي أجهزة الاستخبارات؟
١٢	أجهزة الاستخبارات في المجتمعات الديمقراطية
١٢	ما هو دور أجهزة الاستخبارات المدنية في المجتمع الديمقراطي؟
١٢	ما هو دور أجهزة الاستخبارات العسكرية؟
١٢	الإطار القانوني لأجهزة الاستخبارات
١٢	كيف تضع المجتمعات الديمقراطية الأساس القانوني لأجهزة الاستخبارات؟
١٤	لماذا تحتاج أجهزة الاستخبارات إلى أساس قانوني؟
١٤	هل قوانين الاستخبارات سرية؟
١٥	ما المجالات التي تغطيها قوانين الاستخبارات؟
١٥	كيف تضمن المجتمعات الديمقراطية أن أجهزة الاستخبارات تدعم القانون
١٦	ما هي المعايير القانونية الدولية المرشدة لأجهزة الاستخبارات؟
١٦	هل يجوز لأجهزة الاستخبارات انتهاك حقوق الإنسان؟
١٨	جمع المعلومات
١٨	كيف تقوم الاستخبارات بجمع المعلومات؟
١٨	ما هي المعلومات المسموح لأجهزة الاستخبارات بجمعها؟
١٨	ما هي المعلومات غير المسموح لأجهزة الاستخبارات بجمعها؟
١٩	لماذا تقيد الدول الديمقراطية جمع المعلومات من مهن معينة؟
١٩	كيف يحكم المجتمع الديمقراطي استخدام الصلاحيات الخاصة؟
١٩	من الذي يجيز استخدام الصلاحيات الخاصة؟
٢٠	كيف تصرح الدولة باستخدام الصلاحيات الخاصة؟
٢٠	كيف تشرف المجتمعات الديمقراطية على استخدام الصلاحيات الخاصة؟

## استخدام وإدارة البيانات الشخصية

- ٢٠ ما هي البيانات الشخصية؟
- ٢٠ كيف تحصل أجهزة الاستخبارات على البيانات الشخصية؟
- ٢٢ كيف تستخدم أجهزة الاستخبارات وحكوماتها البيانات الشخصية؟
- ٢٢ لماذا تقيّد المجتمعات الديمقراطية استخدام المعلومات الشخصية؟
- ٢٣ ما هي الضوابط القانونية التي تنطبق على استخدام البيانات الشخصية؟
- ٢٤ من الذي يشرف على استخدام البيانات الشخصية وما هي مهمته؟
- ٢٤ هل يمكن للأفراد الوصول إلى بياناتهم الشخصية؟

## التعاون الدولي في مجال الاستخبارات

- ٢٥ ما هو التعاون الدولي في مجال الاستخبارات؟
- ٢٦ لماذا تتعاون أجهزة الاستخبارات مع الحكومات وأجهزة الاستخبارات الأجنبية؟
- ٢٦ ما هي مخاطر التعاون في مجال الاستخبارات؟
- ٢٦ كيف تراقب الدول التعاون الدولي في مجال الاستخبارات؟
- ٢٦ ما هي الضوابط المطبقة على تبادل المعلومات مع أجهزة الاستخبارات الأجنبية؟
- ٢٨ كيف يتم الإشراف على التعاون الدولي في مجال الاستخبارات؟

## استخدام أجهزة الاستخبارات لصلاحيات الاعتقال والاحتجاز

- ٢٨ هل من المناسب منح أجهزة الاستخبارات صلاحيات اعتقال واحتجاز الأفراد؟
- ٢٨ ما هي المعايير الدولية المطبقة على استخدام صلاحيات الاعتقال والاحتجاز؟
- ٣١ هل أجهزة الاستخبارات بحاجة إلى مراكز احتجاز خاصة بها؟

## استخدام القوة المميتة من قبل أجهزة الاستخبارات

- ٣١ هل يسمح لأجهزة الاستخبارات بالقتل؟

## الرقابة والإشراف على أجهزة الاستخبارات

- ٣١ لماذا تمارس المجتمعات الديمقراطية الرقابة على أجهزة الاستخبارات الخاصة بهم؟
- ٣٢ ما هي المؤسسات التي تراقب و / أو تشرف على أجهزة الاستخبارات؟

## الإدارة الداخلية

٣٣

ما هو الدور الذي تؤديه الإدارة الداخلية في الرقابة على أجهزة الاستخبارات؟

٣٣

لمن ترفع أجهزة الاستخبارات تقاريرها؟

٣٣

من الذي يعين مديري الاستخبارات؟

٣٣

لماذا يتم تعيين مديري الاستخبارات لمدة محددة؟

٣٣

## السلطة التنفيذية

٣٣

ما هو دور السلطة التنفيذية في الرقابة على أجهزة الاستخبارات؟

٣٣

## السلطة القضائية

٣٤

ما هو دور السلطة القضائية في الرقابة على أجهزة الاستخبارات والإشراف عليها؟

٣٤

## البرلمان

٣٤

ما هو دور البرلمان في الرقابة على أجهزة الاستخبارات والإشراف عليها؟

٣٤

## جهات الإشراف ذات الخبرة

٣٥

ما هو دور جهات الإشراف ذات الخبرة على أجهزة الاستخبارات؟

٣٥

## دراسة متعمقة لجهات الإشراف البرلمانية وذات الخبرة على أجهزة الاستخبارات

٣٥

ما هي جوانب العمل الاستخباراتي التي ينبغي الإشراف عليها بواسطة جهات الإشراف البرلمانية و / أو الجهات ذات الخبرة؟

٣٥

ما هي السلطات القانونية المكفولة للهيئات الإشرافية؟

٣٩

لماذا تحتاج هيئات الإشراف إلى موارد مالية وبشرية؟

٣٩

كيف يراقب المشرفون أجهزة الاستخبارات؟

٣٩

كيف تقدم جهات الإشراف تقارير عن أنشطتها؟

٤٠

لماذا تعتبر التقارير العامة أمراً هاماً؟

٤٠

هل هناك تضارب بين الحق في المعرفة والحاجة للحفاظ على سرية المعلومات؟

٤٠

كيف يمكن التوفيق بين احتياجات جهات الإشراف والاستخبارات؟

٤١

ما هي أهمية العلاقة بين أجهزة الاستخبارات وهيئات الإشراف؟

٤١

كيف تضمن المجتمعات الديمقراطية استقلالية هيئات الإشراف على الاستخبارات؟

٤١

كيف يمكن ضمان استقلال أعضاء هيئات الإشراف؟

٤٢

ما هي مزايا هيئات الإشراف البرلمانية؟

٤٢

ما هي مزايا هيئات الإشراف ذات الخبرة؟

٤٣

## الشكاوى ضد أجهزة الاستخبارات

٤٣

كيف يمكن للجمهور التقدم بشكاوى ضد أجهزة الاستخبارات؟

٤٣

ما هي المؤسسات التي تنظر الشكاوى ضد أجهزة الاستخبارات؟

٤٥

لماذا تخطر بعض الدول الأشخاص حال استخدام صلاحيات خاصة ضدهم؟

٤٥

ما الذي يجعل هيئة نظر الشكاوى فعالة؟

٤٥

٤٧

قراءات أخرى

٤٨

ملاحظات ختامية

## قائمة الجداول والمربعات

- جدول ١: أمثلة لصلاحيات ومهام أجهزة الاستخبارات ١٣
- جدول ٢: مقارنة بين هيئات إشرافية استخباراتية مختارة في بلجيكا وكندا وجنوب أفريقيا والمملكة المتحدة ٣٦
- مربع ١: الأحكام الدستورية في جنوب أفريقيا بشأن أجهزة الاستخبارات والأمن ١٤
- مربع ٢: مقتطف من المادة ٣ المشتركة في اتفاقيات جنيف ١٧
- مربع ٣: عملية التصريح باستخدام صلاحيات خاصة من قبل جهاز الاستخبارات الأمنية الكندي ٢١
- مربع ٤: لوائح استخدام البيانات الشخصية من قبل المكتب الاتحادي الألماني لحماية الدستور ٢٣
- مربع ٥: القانون الألماني بشأن إمكانية الوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات ٢٥
- مربع ٦: اللوائح الكرواتية المتعلقة بالتعاون الاستخباراتي مع كيانات أجنبية ٢٧
- مربع ٧: المعايير الدولية المتعلقة بالاعتقال والاحتجاز ٢٩
- مربع ٨: المعايير الدولية بشأن استخدام القوة من جانب الموظفين الحكوميين ٣٢
- مربع ٩: التعامل مع الشكاوى بواسطة لجنة مراجعة الاستخبارات الأمنية الكندية مراجعة الاستخبارات (SIRC) ٤٤
- مربع ١٠: القانون الألماني بشأن إبلاغ الأفراد بعد استخدام سلطات خاصة ضدهم ٤٦



## مقدمة الرزمة

على صياغة تشريعات جديدة. وفي سبيل هذه الغاية، قرر الخبراء العرب والخبراء العاملون في مركز جنيف للرقابة الديمقراطية على القوات المسلحة العمل بدأً من أجل إعداد بعض الأدوات العملية التي تسد الفراغ القائم في هذا الجانب.

### لمن أُعدَّ هذا الدليل الإرشادي؟

يستهدف هذا الدليل الإرشادي بصورة رئيسية جميع الجهات والأشخاص العاملين في المنطقة العربية والذين يسعون إلى إعداد تشريعات ناظمة للقطاع الأمني أو تطوير التشريعات الأمنية القائمة. ويضم هؤلاء البرلمانيين، والموظفين العموميين، والخبراء القانونيين والمنظمات غير الحكومية. وهو على هذه الشاكلة مفيد للمسؤولين الأمنيين، ولا يستغني عنه الباحثون والطلاب المهتمون بالتشريعات التي تحكم القطاعات الأمنية باعتباره أداة مرجعية هامة.

### علام يحتوي هذا الدليل الإرشادي؟

تتضمن مجموعة الأدوات عدد من الكتيبات الموضوعية باللغتين العربية والانكليزية، وتقدّم معايير وقواعد وإرشادات، بالإضافة إلى أمثلة عملية لبعض القوانين النموذجية في مجالات عدة تقع ضمن تشريع القطاع الأمني.

وقد تمّ نشر بعض هذه الأجزاء، في حين ما زال البعض الآخر قيد الإنجاز:

- تشريع الشرطة
- تشريع المخابرات
- تشريع العدالة العسكرية
- اتفاقات مركز القوات

سوف يتم إضافة سلسلة جديدة عند الحاجة، ولا شك في إمكانية زيادة السلسلة الحالية بإضافة كتيبات جديدة وفقاً لما تقتضيه الحاجة في المنطقة العربية.

للإطلاع على أحدث المؤلفات والمنشورات الصادرة في هذا الشأن، يرجى زيارة الموقع الإلكتروني:

[www.dcaf.ch/publications](http://www.dcaf.ch/publications)

يمثل سنّ التشريعات الناظمة للقطاع الأمني عملية صعبة ومعقدة. ولذلك، يجد العديد من المشرّعين أن من السهل نسخ تشريعات واستيرادها من بلاد أخرى؛ فهذا يسرّع هذا الأمر من عملية الصياغة، ولا سيما عندما تتوفر النصوص التشريعية المطلوبة في لغة المشرع نفسه. ولكن النتيجة المترتبة على ذلك تتمثل في معظم الحالات في إخراج تشريعات ضعيفة وركيكة.

وغالباً ما تعتبر القوانين المنسوخة، حتى بعد تعديلها، قديمة قبل أن تدخل حيز النفاذ والسريان؛ فلا تعود هذه القوانين تتماشى مع المعايير الدولية ذات الصلة أو أنها لا تلبي الاحتياجات التي يستدعيها السياق السياسي والاجتماعي المحلي. وفي بعض الأحيان، ينعدم الانسجام بين تلك القوانين المنسوخة والتشريعات الوطنية النافذة.

في بعض الحالات، قد لا يتوفر في المنطقة المعنية قانون نموذجي يمكن المشرّعين من إعداد التشريع المطلوب على غرار. وقد كانت هذه هي الحالة القائمة في المنطقة العربية التي لا يزال الحوار العام الذي نشأ فيها حول القطاع الأمني في مهده. ولذلك، فمن الصعب العثور على نماذج جيدة من القوانين التي تنظم عمل أجهزة الشرطة بصورة ديموقراطية أو رقابة البرلمان على أجهزة المخابرات مثلاً.

لذا، لا يستغرب المرء أن يرى العديد من المشرّعين العرب وقد اعتراهم الإحباط والتخبط والعجز أمام المهمة الموكلة إليهم في صياغة التشريعات الناظمة لقطاع الأمن؛ فقد ألقى هؤلاء المشرّعون أن من العسير عليهم الإطلاع على المعايير والقواعد الدولية ذات العلاقة بسبب ندرة المصادر المتوفرة باللغة العربية أو انعدامها بالكامل. كما لم يعرف الكثير منهم أين يمكنهم العثور على قوانين نموذجية، وأوشك عدد آخر منهم على التسليم بالأمر الواقع وترك العمل في هذا المجال. وفي نهاية المطاف، لجأ بعض المشرّعين إلى مركز جنيف للرقابة الديمقراطية على القوات المسلحة طلباً للمساعدة في هذا الشأن.

لقد خرجت فكرة إعداد دليل إرشادي للجهات التشريعية في المنطقة العربية إلى النور بسبب غياب المصادر التشريعية الضرورية؛ فقد كان العاملون في مجال إعداد التشريعات وصياغتها يبحثون عن مجموعة منتقاة من المعايير والقواعد والقوانين النموذجية المكتوبة باللغة العربية والتي تساعدهم

### ما الهدف من هذا الدليل الإرشادي؟

يسعى هذا الدليل الإرشادي إلى مساعدة المشرّعين في المنطقة العربية على تلبية احتياجات مواطنيهم والارتقاء إلى مستوى توقعاتهم. ففي الواقع، يتطلع المواطنون العرب إلى تلقي خدمات مهنية من أجهزة الشرطة وقوى الأمن العاملة في مجتمعاتهم، والتي يتحتم عليها أن تثبت فعاليتها وتأثيرها وأن تؤمّن احتياجات المواطنين. كما يتوقع المواطنون العرب من أجهزة الشرطة والأجهزة الأمنية وعناصرها الالتزام بالقانون وبمعايير حقوق الإنسان، بالإضافة إلى خضوعهم للمساءلة عن أداؤهم وسلوكهم. ولذلك، يعمل هذا الدليل الإرشادي على ترسيخ المعايير الدولية في التشريعات الناظمة للقطاع الأمني، من قبيل الرقابة الديموقراطية، والحكم الرشيد والشفافية.

وعلاوةً على ما تقدم، يستعرض هذا الدليل الإرشادي، بنسخته العربية والإنجليزية، القواعد الدولية جنباً إلى جنب مع أمثلة على تشريعات من خارج المنطقة العربية، وهو ما يتيح الفرصة للمقارنة بين مختلف التجارب والممارسات في هذا المجال.

لقد أفرزت ندرة الأدبيات المنشورة باللغة العربية حول التشريعات الأمنية مشكلة كبيرة أمام المشرّعين العرب. وفي هذا الصدد، يهدف هذا الدليل إلى سدّ هذه الفجوة. ويتمثل أحد الأهداف التي يسعى الدليل إلى تحقيقها في تقليص الوقت الذي يُضفيه المشرّعون في البحث عن المعلومات، مما يسمح لهم بالتركيز على المهمة الرئيسية التي ينكبّون على إنجازها. ومع توفر قدر أكبر من المعلومات باللغة العربية، فقد يسهّل على العديد من المواطنين ومؤسسات المجتمع المدني أن يعبروا عن رؤيتهم لنوع أجهزة الشرطة وقوى الأمن التي يريدونها، كما يمكنهم المساهمة في إعداد إطار قانوني حديث وقوي لتنظيم القطاع الأمني.

### لماذا تدعو الحاجة إلى إعداد إطار قانوني حديث وقوي للقطاع الأمني؟

يمثل الإطار القانوني السليم شرطاً ضرورياً مسبقاً لضمان الحكم الرشيد للقطاع الأمني الذي يتّسم بفعاليتها ونجاعته وخضوعه للمساءلة، وذلك للأسباب التالية:

- يحدد هذا الإطار القانوني دور مختلف الأجهزة الأمنية والمهام الموكلة لكل منها.
- ويحدد الامتيازات الممنوحة لأجهزة الأمن ولأفرادها والقيود المفروضة على صلاحياتهم.

- ويحدد دور وصلاحيات المؤسسات التي تدير الأجهزة الأمنية وتفرض الرقابة عليها.
  - ويوفر هذا الإطار القاعدة اللازمة لإجراء المساءلة، حيث أنه يضع حداً فاصلاً واضحاً بين السلوك القانوني والسلوك غير القانوني.
  - كما يعزز هذا الإطار الثقة العامة ويرسّخ شرعية الحكومة وقوى الأمن التابعة لها في نظر المواطنين.
- ولهذه الأسباب مجتمعة، غالباً ما تُستهل عملية إصلاح القطاع الأمني بمراجعة شاملة للتشريعات الوطنية التي تنظم هذا القطاع وإعادة صياغتها. وفي هذا السياق، تركز هذه المهمة على تحديد ومعالجة مواطن التعارض وغياب الوضوح الذي يكتنف أدوار المؤسسات الأمنية المختلفة وصلاحياتها.

## فهم الاشراف على الاسخبارات

### من المستهدف بهذا الدليل؟

هذا الدليل هو للمهتمين بإدارة أجهزة الاستخبارات، ولكن في نفس الوقت يفكرون إلى الإلمام التام بهذا الموضوع. وبشكل أكثر تحديدا، يستهدف هذا الدليل ثلاث مجموعات رئيسية: أولا، المعنيين بوضع القوانين والجوانب المؤسسية الحاكمة لأجهزة الاستخبارات، بما في ذلك البرلمانين والعاملين بالبرلمانات وأعضاء السلطة التنفيذية والموظفين في دوائر الاستخبارات وممثلي منظمات المجتمع المدني. ثانيا، الأعضاء والعاملين في هيئات الإشراف التي أنشئت حديثا. وأخيرا، يسعى هذا الدليل إلى تلبية احتياجات المعلمين والطلاب ممن يرغبون في الحصول على معلومات عامة عن إدارة الاستخبارات.

تم تقديم مواد هذا الدليل بطريقة وصفية في شكل سلسلة من الأسئلة والأجوبة البسيطة، وهو ما من شأنه مساعدة الممارسين غير الخبراء في تطبيق واستخدام المواد حسب احتياجاتهم.

### ما هي أجهزة الاستخبارات؟

يشير هذا الدليل إلى أجهزة الاستخبارات بوصفها منظمات حكومية تتمثل مهامها الرئيسية في جمع وتحليل المعلومات ذات الصلة بالأمن القومي ونشرها لصناع القرار. وتتعلق هذه المعلومات أساسا بما يمثل تهديدا للأمن القومي، مثل الإرهاب وانتشار أسلحة الدمار الشامل والتجسس من قبل الدول المعادية.

في معظم الدول الديمقراطية، يتم تنفيذ هذه المهام من قبل جهاز استخبارات متخصص. ومع ذلك، هناك بعض البلدان توكل القيام بهذه المهام لهيئة من هيئات الشرطة.

كثيرا ما تسمح الدول لأجهزة استخباراتها بالعمل حصريا داخل أو خارج حدود الدولة، وبالتبعية، قد يكون لدى الدول أجهزة استخبارات مختلفة للعمل داخل وخارج الحدود الوطنية. وهناك دول أخرى تكلف جهاز استخبارات واحد بالعمل داخل وخارج حدود البلاد. وفي حين أن هذا الدليل يركز في المقام الأول على أجهزة الاستخبارات الداخلية، المعروفة بأجهزة الاستخبارات التي تعمل داخل أراضي الدولة، إلا أن المبادئ الأساسية للإشراف والرقابة تنطبق على أجهزة الاستخبارات التي تعمل خارج الدولة كذلك.

### ما هو الهدف من هذا الدليل؟

يعتبر هذا الدليل بمثابة مقدمة للدول الديمقراطية بشأن كيفية إدارة أجهزة استخباراتها، فضلا عن توضيحه لسبل إدارة هذه الأجهزة للتأكد من أنها:

- أ. تسهم بشكل فعال في الحفاظ على أمن الدولة وأمن سكانها
- ب. تخضع للرقابة الديمقراطية
- ج. مسؤولة أمام السكان الذين تخدمهم
- د. تحترم سيادة القانون وحقوق الإنسان.

يقدم الدليل إجابات مختصرة وبسيطة على الأسئلة المتداولة حول أنشطة أجهزة الاستخبارات، فضلا عن الرقابة والإشراف على هذه المنظمات. كما أنه يعتمد بشكل كبير على القوانين، والنماذج والممارسات المؤسسية لمجموعة كبيرة من الدول الديمقراطية. كما يوضح هذا الدليل أيضا أن الدول الديمقراطية تختلف في نهجها لتنظيم وتحديد مهام أجهزة الاستخبارات والإشراف عليها، حيث لا يوجد نموذج أو نهج أوحده «صحيح». وما سبق لا يمس بحقيقة أن هناك قبولا واسع النطاق لممارسات جيدة حيال أنشطة وخدمات الإشراف على أجهزة الاستخبارات تُطبق في العديد من الدول الديمقراطية - يبين هذا الدليل العديد منها.

### ما الذي يحتويه هذا الدليل؟

ينقسم الدليل إلى سبعة أقسام. يركز القسم الأول منها على الدور الذي تؤديه أجهزة الاستخبارات في المجتمعات الديمقراطية، بينما يتناول القسم التالي بعض السمات الرئيسية للأطر القانونية التي تنظم أجهزة الاستخبارات. وقد خُصصت أربعة أقسام لشرح كيفية مراقبة الدول الديمقراطية لأنشطة الاستخبارات في جمع المعلومات الاستخباراتية واستخدام وإدارة البيانات الشخصية والتعاون الدولي. ويأتي القسم الأخير من هذا الدليل ليركز على الرقابة والإشراف على أجهزة الاستخبارات من جانب السلطة التنفيذية والبرلمان والقضاء وهيئات الإشراف ذات الخبرة.

## أجهزة الاستخبارات في المجتمعات الديمقراطية

### ما هو دور أجهزة الاستخبارات المدنية في المجتمع الديمقراطي؟

تعد أجهزة الاستخبارات جزءاً هاماً من قطاع الأمن في المجتمع الديمقراطي. حيث تتمثل مهمتها الأساسية في جمع وتحليل المعلومات حول التهديدات الموجهة ضد الدولة وسكانها وتقوم بتقديم هذه المعلومات للحكومة، مما يمكنها من وضع وتنفيذ السياسة الأمنية. ومع ذلك، فإن أجهزة الاستخبارات ليست مسئولة عن تنفيذ السياسة الأمنية، إذ أن ذلك يقع على عاتق الشرطة وبقية هيئات إنفاذ القانون الأخرى.

كذلك فإن دور أجهزة الاستخبارات في جمع المعلومات محدود وتركز في تحقيقاتها على الأنشطة التي تشكل تهديداً للأمن القومي. وتقوم بذلك وفقاً للتشريعات والتوجيهات السياسية للحكومة. وفي هذا السياق يستمد تعريف ما يشكل تهديداً للأمن القومي من المجتمع وليس من أجهزة الاستخبارات. وعادة ما تكون هذه العملية عملية مطولة ينتج عنها صياغة سياسة أو تشريعات الأمن القومي.

تتولى أجهزة الاستخبارات مهاماً أخرى بالإضافة إلى دورها في جمع المعلومات، منها على سبيل المثال أنشطة مكافحة التجسس. وتشمل هذه الأنشطة كشف ووقف أعمال التجسس التي تجريها أجهزة الاستخبارات الأجنبية ضد مصالح الدولة وسكانها. بالإضافة إلى ذلك، غالباً ما تكون أجهزة الاستخبارات مسئولة عن حماية المعلومات ونظم المعلومات في الدولة. فعلى سبيل المثال، تقوم هذه الأجهزة بتصفية المتقدمين للوظائف الحكومية التي من شأنها تمكين هؤلاء الأفراد من الوصول إلى معلومات سرية. (انظر جدول ١ لمزيد من التفاصيل حول اختصاصات ومهام بعض أجهزة الاستخبارات المختارة).

ومن هنا نرى أن دور الاستخبارات ضروري لحماية الدولة والسكان. ويحظر القانون الوطني على أجهزة الاستخبارات تعزيز أو حماية المصالح الخاصة بأي جماعة إثنية أو دينية أو غيرها. ومن هنا تظل هذه الأجهزة محايدة في دورها في خدمة جميع الأفراد في المجتمع. ومن خلال منعها الإرهاب والتهديدات الأخرى للأمن الوطني، تسهم الاستخبارات في سلامة ورفاهية جميع الأفراد في المجتمع.

### ما هو دور أجهزة الاستخبارات العسكرية؟

تمثل أجهزة الاستخبارات العسكرية أو الدفاعية جزءاً من القوات المسلحة. وتكون صلاحيات هذه الأجهزة في المجتمعات الديمقراطية أكثر محدودية من تلك المخولة لأجهزة الاستخبارات المدنية. فهي مسئولة أساساً عن جمع وتحليل المعلومات حول التهديدات التي يتعرض لها أفراد القوات المسلحة وقواعدها وتبادل هذه المعلومات مع القيادة العسكرية العليا والقيادة السياسية. وقد تنبع التهديدات المحتملة التي يتعين على الاستخبارات العسكرية رصدها من داخل القوات المسلحة أو الجماعات المحلية أو من الدول والكيانات الأجنبية. وفي دول كثيرة، يتم تكليف أجهزة الاستخبارات العسكرية أيضاً بحماية المعلومات الحساسة المتعلقة بالدفاع ونظم الاتصالات. وقد تعمل الاستخبارات العسكرية في الداخل والخارج اعتماداً على احتياجات البلاد وتشريعاتها ونشر قواتها.

وفي هذا السياق، لا تسمح المجتمعات الديمقراطية لأجهزة الاستخبارات العسكرية بجمع المعلومات حول التهديدات التي يتعرض لها الأمن طالما أنها ليست ذات صلة بعمليات الدفاع، حيث إن مسؤولية جمع المعلومات عن التهديدات غير العسكرية تقع على عاتق أجهزة الاستخبارات المدنية. ومن هنا، فإن أجهزة الاستخبارات العسكرية لا يُسمح لها عادة بجمع المعلومات عن المدنيين في دولتهم. وفي كثير من الدول، يتطلب القانون من أجهزة الاستخبارات العسكرية اللجوء إلى جهاز الاستخبارات المدنية إذا كانت بحاجة إلى جمع معلومات حول تهديدات تواجه القوات المسلحة على يد مدنيين. وقد تم وضع هذا القيد خصيصاً لمنع القوات المسلحة من التدخل في الشؤون المدنية.

## الإطار القانوني لأجهزة الاستخبارات

### كيف تضع المجتمعات الديمقراطية الأساس القانوني لأجهزة الاستخبارات؟

تدرج بعض الدول الديمقراطية أحكاماً عامة بشأن أجهزة الاستخبارات في دساتيرها. وعادة ما تكون هذه القواعد الدستورية أحكاماً عامة، مثل إخضاع هذه الأجهزة للمساءلة أمام البرلمان واحترامها لسيادة القانون. (انظر مربع ١ للإطلاع على الأحكام الدستورية في جنوب أفريقيا بشأن أجهزة الاستخبارات والأجهزة الأمنية).

جدول ١: أمثلة لصلاحيات ومهام أجهزة الاستخبارات<sup>١</sup>

البلد	صلاحيات ومهام أجهزة الاستخبارات المدنية
كندا	<p>يقوم جهاز الاستخبارات بجمع المعلومات، من خلال التحقيقات أو أي وسائل أخرى حسبما تقتضي الضرورة القصوى، وتحليلها والاحتفاظ بها وكذلك الاستخبارات ذات الصلة بالأنشطة التي تتوافر أسباب معقولة للاشتباه في تشكيلها تهديدات لأمن كندا، ويقوم برفع تقارير عنها وتقديم المشورة اللازمة للحكومة الكندية».</p> <p>يجوز لجهاز الاستخبارات تقديم تقييمات أمنية إلى الإدارات التابعة لحكومة كندا. يجوز لجهاز الاستخبارات:</p> <p>أ. تقديم المشورة لأي وزير في المسائل المتعلقة بأمن كندا، أو</p> <p>ب. تزويد أي وزير بالمعلومات المتعلقة بالمسائل الأمنية أو الأنشطة الإجرامية ذات الصلة بممارسة أي سلطة أو أداء أي واجب أو وظيفة من قبل هذا الوزير بموجب قانون المواطنة أو قانون الهجرة وحماية اللاجئين.</p>
كرواتيا	<p>جمع وتحليل ومعالجة وتقييم المعلومات ذات الصلة بالأمن القومي دورياً، بهدف كشف ومنع الأنشطة، من قبل أفراد أو جماعات، الموجهة ضد: سلامة واستقلال ووحدة وسيادة جمهورية كرواتيا، والتي تستهدف الإطاحة الجبرية بهيكل سلطة الدولة وتهدد بانتهاك حقوق الإنسان والحريات الأساسية المنصوص عليها في دستور وتشريعات جمهورية كرواتيا، وتعرض أسس النظام الاقتصادي لجمهورية كرواتيا للخطر.</p>
هولندا	<p>إجراء التحقيقات المتعلقة بالمنظمات والأشخاص، بسبب الأهداف التي يسعوا لتحقيقها أو من خلال أنشطتهم، الذين يثيرون شكوكاً خطيرة في أنهم يشكلون خطراً على استمرار وجود نظام قانوني ديمقراطي، أو على الأمن أو غيرها من المصالح الحيوية للدولة.</p> <p>إجراء تحقيقات السلامة الأمنية على النحو المشار إليها في قانون التحقيقات الأمنية؛ تعزيز التدابير [...] لحماية المعلومات التي ينبغي الحفاظ على سريتها لأسباب تتعلق بالأمن القومي والمعلومات المتعلقة بخدمات عامة ودوائر أعمال التي يرى الوزراء المعنيون أنها ذات أهمية حيوية لاستقرار النظام الاجتماعي؛</p> <p>إجراء التحقيقات بشأن البلدان الأخرى حيال موضوعات معينة يحددها رئيس الوزراء، وزير الشؤون العامة، وفقاً للمشاورات مع الوزراء المعنيين.</p>

ترجع أهمية الأساس القانوني إلى أربعة أسباب رئيسية.

**فأولاً،** ينص القانون بشكل واضح على اختصاصات وأدوار ومسؤوليات أجهزة الاستخبارات ومسئولياتها، فضلاً عن تحديده أيضاً للأنشطة المسموح لتلك الأجهزة بتأديتها. وتعتمد الحكومات على القانون في تنظيم أجهزة الاستخبارات.

**ثانياً،** يعتبر الأساس القانوني لجميع المؤسسات الحكومية أمراً ضرورياً لتعزيز الشفافية، حيث تطلع القوانين العامة المجتمع على مهام وسلطات الحكومة. ومن هنا كان لأجهزة الاستخبارات أساس قانوني للاضطلاع بسلطات خاصة لجمع المعلومات التي لا تتوفر عادة لأفراد أو جهات حكومية أخرى. على سبيل المثال، قد تسمح القوانين باستخدام تدابير خاصة للتحقيق مع الأفراد في الوقت الذي يحتاج فيه هؤلاء الأفراد إلى معرفة مدى تأثير أجهزة الاستخبارات على حياتهم الشخصية وعمّا إذا كان ضباط الاستخبارات يحترمون حقوق الأفراد المكفولة بموجب القانون أم لا.

**ثالثاً،** إن وجود أساس قانوني من شأنه أن يكسب أجهزة الاستخبارات الشرعية في أعين الجمهور. وكذلك وجود قانون متاح للجمهور يشجع على فهم أدوار أجهزة الاستخبارات وسبب احتياجها لأموال عامة لتنفيذ المهام المنوطة بها، فضلاً عن إمكانية مساعدته على ضمان دعم الجمهور لأجهزة الاستخبارات.

**وأخيراً،** هناك حاجة لتضمين قوانين الاستخبارات العامة ما يكفل مساءلة الحكومة. ومن هنا فإن الجهات الرقابية بالاستخبارات والجمهور بصفة عامة تخضع الأجهزة التنفيذية وأجهزة الاستخبارات للمساءلة من حيث امتثالها لهذه القوانين. كذلك فإن القوانين العامة تمكن الأفراد من السعي لتحقيق العدالة متى اعتقدوا قيام الاستخبارات بأعمال غير مشروعة ضدهم.

### هل قوانين الاستخبارات سرية؟

في الدول الديمقراطية توجد القوانين الأساسية التي تحكم أجهزة الاستخبارات في المجال العام. وكما أوضح النقاش أعلاه، فإن الجمهور بحاجة إلى معرفة أدوار أجهزة الاستخبارات وما هي الصلاحيات التي تتمتع بها لأداء هذه المهام. كذلك يحتاج الجمهور إلى معرفة وقت وشروط السماح لأجهزة الاستخبارات بتقييد الحقوق الفردية لأغراض الأمن القومي. ولذلك لا بد أن تنص القوانين العامة على سلطة أجهزة الاستخبارات في تقييد حقوق الإنسان.

بالإضافة إلى ذلك، فإن معظم الدول الديمقراطية تطبق تشريعاً خاصاً بأجهزة الاستخبارات يمثل الأساس القانوني الرئيسي لتنظيم أنشطة أجهزة الاستخبارات. كذلك تمثل قوانين احترام الخصوصية وحماية البيانات وأمن المعلومات والوصول إلى المعلومات أدوات تنظيمية هامة لأجهزة الاستخبارات. وعلى رأس ذلك تأتي المسائل التنفيذية أو ما يسمى بـ «الأوامر التنفيذية» (التوجيهات) واللوائح الأخرى المكملة للتشريعات. فهذه اللوائح تعتمد دوماً على التشريعات الحالية ومن ثم يتعين الامتثال لها.

### مربع ١: الأحكام الدستورية في جنوب أفريقيا بشأن أجهزة الاستخبارات والأمن<sup>٢</sup>

يضم دستور جمهورية جنوب أفريقيا عدداً من الأحكام العامة بشأن أجهزة الاستخبارات والأمن.

- يتعين الحفاظ على الأمن القومي في ضوء الامتثال للقانون، بما في ذلك القانون الدولي.
- يخضع الأمن القومي لسلطة البرلمان والسلطة التنفيذية الوطنية.
- يتعين هيكلة وتنظيم الأجهزة الأمنية بموجب تشريعات وطنية.
- يتعين على الأجهزة الأمنية أن تعمل وتعلم وتطلب من أعضائها العمل وفقاً للدستور والقانون، بما في ذلك القانون الدولي العرفي والاتفاقات الدولية الملزمة للجمهورية.
- لا يجوز للأجهزة الأمنية، ولا أي من أعضائها، أثناء أداء وظائفها أن:

أ. تمس بمصلحة حزب سياسي شرعي بموجب

أحكام الدستور، أو

ب. تعزز، بطريق التأييد، أي مصلحة لحزب سياسي.

لتفعيل مبادئ الشفافية والمساءلة، يتعين السماح للجان برلمانية تضم أحزاب متعددة بالإشراف على جميع الأجهزة الأمنية بطريقة تحددها التشريعات الوطنية أو القواعد والأوامر الصادرة عن البرلمان.

يجب أن تنظم التشريعات الوطنية شئون ووظائف وسلطات أجهزة الاستخبارات.

### لماذا نحتاج أجهزة الاستخبارات إلى أساس قانوني؟

تعكف المجتمعات الديمقراطية على التأكد من أن أجهزة الاستخبارات تعمل وفقاً للقوانين الوطنية. وفي هذا السياق

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

الحكومية وغير الحكومية بالإشراف على أجهزة الاستخبارات. على سبيل المثال، تنظم هذه القوانين عملية تعيين كبار مديري الاستخبارات وتحدد اختصاصات وصلاحيات هيئات الرقابة البرلمانية وذات الخبرة.

خامسا، تصف قوانين الاستخبارات العلاقات المهنية بين أجهزة الاستخبارات وغيرها من المنظمات الحكومية وغير الحكومية والمنظمات الدولية. على سبيل المثال، تصف قوانين الاستخبارات العمليات المستخدمة لتبادل المعلومات أو إجراء عمليات مشتركة مع المنظمات الأخرى.

سادسا، كثيرا ما توفر قوانين الاستخبارات لوائح إرشادية حول كيفية استخدام البيانات الشخصية من قبل أجهزة الاستخبارات (انظر صفحة ٢٠-٢٥).

وأخيرا، تصف قوانين الاستخبارات العمليات التي ينتهجها الأفراد حال رغبتهم في تقديم شكاوى حول الإجراءات الاستخباراتية المتخذة ضدهم (انظر صفحة ٤٣-٤٥).

### كيف تضمن المجتمعات الديمقراطية أن أجهزة الاستخبارات تدعم القانون

يتعين على أجهزة الاستخبارات، تماما كما هو الحال مع كل الوكالات الحكومية الأخرى، احترام القانون الدولي والوطني مع إيلاء أهمية خاصة لأحكام القانون الدولي لحقوق الإنسان والقانون الإنساني الدولي. ويجب أن يكون القانون الوطني للدولة والمعني بأجهزة الاستخبارات متسقا مع التزاماتها القانونية الدولية.

كذلك يتعين على كل أجهزة الاستخبارات والعاملين بها الالتزام بالقانون، وهو ما ينطبق أيضا على السلطة التنفيذية حيث لا يجوز للسلطات السياسية إصدار أوامر إلى أجهزة الاستخبارات تتطلب منها اتخاذ إجراءات غير قانونية.

يعتبر أعضاء السلطة التنفيذية من الناحية القانونية مسؤولين عن إصدار توجيهات إلى أجهزة الاستخبارات. بينما يتحمل العاملون في أجهزة الاستخبارات وحدهم مسؤولية ضمان أن الإجراءات الخاصة بهم تمتثل للقانون. في كثير من الدول، لا يتطلب القانون التأكد من امتثال الإجراءات للقانون فقط وإنما يلزم موظفي أجهزة الاستخبارات برفض الأوامر التي من شأنها أن تنتهك القانون الوطني أو الدولي. وهكذا، يتعين على كل عضو في أجهزة الاستخبارات تحمل مسؤولية سلوكه غير القانوني وقد يتعرض في هذا الصدد إلى ملاحقة قانونية حتى وإن كان ذلك السلوك تنفيذا لأمر من رئيسه. ونظرا للصلاحيات الواسعة التي يمكن إعطاؤها

وعلى الرغم من ذلك، يجوز للحكومة إصدار «لوائح فرعية» - مثل «المراسيم» و«التعليمات الوزارية» - لا تتاح للجمهور. ويخول القانون الحكومة إصدار مثل هذه اللوائح حال اعتقادها أن إتاحة معلومات محددة للجمهور يمكن أن يعرض عمل أجهزة الاستخبارات و / أو الأمن القومي بشكل عام للخطر. وعادة ما تحتوي اللوائح غير المتاحة للجمهور على المعلومات المتصلة بالأساليب التنفيذية لأجهزة الاستخبارات، مثل استخدامها لأجهزة أو تقنيات خاصة. غالبا ما يتم الإبقاء على سرية مثل هذه المعلومات لتجنب اكتشاف أجهزة الاستخبارات أو الكشف عن الأشخاص الذين يعملون بها، إذ أن ذلك قد يقوض فعالية أجهزة الاستخبارات ويشكل تهديدا لسلامة العاملين فيها ويمكن أن يضر في نهاية المطاف بالأمن القومي ككل.

وعلى الرغم من عدم إتاحتها للجمهور، إلا أن مثل هذه اللوائح يجب أن تمتثل للقوانين العامة المعمول بها والدستور. على سبيل المثال، لا يمكن السماح لأجهزة الاستخبارات باتخاذ إجراءات تنتهك حقوق الإنسان المكفولة بموجب القانون الدولي.

### ما المجالات التي تغطيها قوانين الاستخبارات؟

تسمح قوانين الاستخبارات للدول بتنظيم والإشراف على أجهزة الاستخبارات. ومن هنا فإن هذه القوانين تغطي المجالات التالية.

أولا، تحدد قوانين الاستخبارات اختصاصات أجهزة الاستخبارات وتقدم قائمة شاملة بمهامها. وعادة ما تحتوي هذه الاختصاصات على تعريفات لما يشكل تهديدا للأمن القومي. وفي نفس الوقت تحد هذه القوانين من دور أجهزة الاستخبارات من حيث منعها ضباط الاستخبارات من تحقيق مصالح أخرى غير تلك الخاصة بالدولة وسكانها.

ثانيا، تقدم قوانين الاستخبارات قائمة شاملة بالصلاحيات المتاحة لأجهزة الاستخبارات وتنظم كيفية استخدامها. وتسمح هذه القوانين لأجهزة الاستخبارات باستخدام هذه الصلاحيات في سياق اختصاصها بينما تحد من استخدام الصلاحيات التي قد تؤدي إلى تقييد الحقوق الفردية لأغراض الأمن القومي.

ثالثا، تصف قوانين الاستخبارات بنية وتكوين أجهزة الاستخبارات بما في ذلك المسؤوليات التنظيمية للإدارات داخل هذه الأجهزة.

رابعا، توضح قوانين الاستخبارات كيفية قيام الكيانات

يتعين على الدول التأكد من تطبيق هذه المعايير القانونية الدولية في قوانينها المحلية.

يحدد القانون الدولي لحقوق الإنسان ثلاث فئات من حقوق الإنسان والحريات:

١. الحقوق التي لا يمكن أبداً الحد أو الانتقاص منها في أي ظرف من الظروف؛
٢. الحقوق التي يمكن الحد منها لأسباب محددة وفقاً لمعايير قانونية صارمة؛
٣. الحقوق التي يمكن تعليقها أو الحد منها خلال النزاع المسلح أو حالات الطوارئ التي تهدد وجود الدولة.

### ١. حقوق الإنسان التي لا يمكن الحد أو الانتقاص منها

يحظر القانون الدولي لحقوق الإنسان على الدول وأجهزتها المعنية الحد أو الانتقاص من حقوق الإنسان في أي ظرف من الظروف. وتشمل هذه الحقوق الحق في الحياة والتحرر من التعذيب وغيره من ضروب المعاملة اللاإنسانية أو المهينة والحق في محاكمة عادلة والحق في الاعتراف أمام القانون والتحرر من الرق والعبودية القسرية وحظر الاختطاف والاحتجاز في أماكن مجهولة<sup>٢</sup>. ويكمل ويعزز القانون الإنساني الدولي هذا الحظر في أوقات النزاع المسلح، حيث تحدد المادة ٣ المشتركة في اتفاقيات جنيف هذه المعايير الدنيا (انظر مربع ٢). ومن ثم لا يجوز لأجهزة الاستخبارات اتخاذ أي إجراء يمس بتلك الحقوق في أي وقت.

### ٢. حقوق الإنسان التي يمكن الحد منها

يجوز القانون الدولي لحقوق الإنسان للدول الحد من بعض حقوق الإنسان وحريات أشخاص معينة. وتشمل هذه الحقوق الحق في الحرية والخصوصية وحرية التنقل وتكوين الجمعيات والتعبير. ويمكن للدول أن تتخذ مثل هذه التدابير التي تحد من ممارسة هذه الحقوق إذا كانت تلك التدابير متوافقة مع المعايير التالية:

١. على أساس قانون عام.
٢. السعي لتحقيق غرض مشروع (مثل حماية الأمن القومي أو السلامة العامة أو حقوق الإنسان وحريات الآخرين).

لأعضاء أجهزة الاستخبارات، تكتسب المسؤولية الفردية أهمية خاصة كضمان ضد الجرائم الخطيرة، بما فيها انتهاكات حقوق الإنسان، مثل التعذيب والقتل خارج نطاق القضاء.

ومن ثم فمن الأهمية بمكان أن يخضع ضباط الاستخبارات، وإذا لزم الأمر، أعضاء السلطة التنفيذية للمساءلة أماما السلطة القضائية بموجب القانون. ويمكن الطعن في قراراتهم وإجراءاتهم الفردية أمام المحكمة، وتكون أحكام المحكمة ملزمة للسلطة التنفيذية، فضلاً عن أجهزة الاستخبارات والموظفين التابعين لها.

## ما هي المعايير القانونية الدولية المرشدة لأجهزة الاستخبارات؟

بوصفها مؤسسة من مؤسسات الدولة، يجب أن تمتثل أجهزة الاستخبارات للالتزامات الدولية والقانونية للحكومة. وفي هذا الصدد، تنطبق التزامات الدولة بموجب القانون الدولي لحقوق الإنسان، ولاسيما الحقوق المدنية والسياسية الواردة في ميثاق الأمم المتحدة والعهد الدولي الخاص بالحقوق المدنية والسياسية، على أجهزة الاستخبارات. وتشمل هذه الحقوق الحق في الحياة والحرية والمحاكمة العادلة والخصوصية وحرية التعبير وتكوين الجمعيات.

كذلك تنطبق المعايير الدولية بشأن أنشطة إنفاذ القانون على أجهزة الاستخبارات إذا كان القانون الوطني يسمح لها بأداء مهام إنفاذ القانون مثل الاعتقال والاحتجاز.

في عام ٢٠٠٩ وعام ٢٠١٠، قامت الأمم المتحدة بمراجعة المعايير الدولية القانونية القائمة والضوابط المؤسسية المنطبقة على أجهزة الاستخبارات. كذلك قرر مجلس الأمم المتحدة لحقوق الإنسان إجراء دراسة «للممارسات الجيدة» حول الأطر المؤسسية القانونية لأجهزة الاستخبارات والجوانب الرقابية ذات الصلة. ضمت هذه الدراسة ٣٥ ممارسة دولية هامة وتم تقديمها إلى مجلس حقوق الإنسان في يونيو ٢٠١٠ (انظر قائمة المراجع).

## هل يجوز لأجهزة الاستخبارات انتهاك حقوق الإنسان؟

يحظر القانون الدولي لحقوق الإنسان على الدول (بما في ذلك أجهزة استخباراتها) انتهاك حقوق الإنسان على يد أي شخص تحت ولايتها. ومثلها مثل كل الوكالات الحكومية، يجب على أجهزة الاستخبارات الالتزام بالقانون الدولي لحقوق الإنسان. وفي حالات النزاع المسلح، يجب على أجهزة الاستخبارات أيضاً الامتثال للقانون الدولي الإنساني، بينما

في حالة قيام نزاع مسلح ليس له طابع دولي [...] يكون كل طرف من أطراف النزاع ملزماً بأن يطبق كحد أدنى الأحكام التالية:

١. الأشخاص الذين لا يشتركون مباشرة في الأعمال العدائية، بمن فيهم أفراد القوات المسلحة الذين ألقوا عنهم أسلحتهم، والأشخاص العاجزون عن القتال بسبب المرض أو الجرح أو الاحتجاز أو لأي سبب آخر، يعاملون في جميع الأحوال معاملة إنسانية، دون أي تمييز ضار يقوم على العنصر أو اللون، أو الدين أو المعتقد، أو الجنس، أو المولد أو الثروة أو أي معيار مماثل آخر.
- ولهذا الغرض، تحظر الأفعال التالية فيما يتعلق بالأشخاص المذكورين أعلاه، وتبقى محظورة في جميع الأوقات والأماكن:
  - أ. لاعتداء على الحياة والسلامة البدنية، وبخاصة القتل بجميع أشكاله، والتشويه، والمعاملة القاسية، والتعذيب،
  - ب. أخذ الرهائن،
  - ج. الاعتداء على الكرامة الشخصية، وعلى الأخص المعاملة المهينة والمذلة،
  - د. إصدار الأحكام وتنفيذ العقوبات دون إجراء محاكمة سابقة أمام محكمة مشكلة تشكيباً قانونياً، وتكفل جميع الضمانات القضائية اللازمة في نظر الشعوب المتمدنة.

توافقها مع المعايير الدولية، حيث تتأكد هذه الدول من أن هذه الصلاحيات منظمة بموجب القانون وتشرف عليها مؤسسات خارج دوائر الاستخبارات (انظر صفحة ١٩-٢١).

٣. أن تكون حتمية في مجتمع ديمقراطي.

٤. متسقة مع الأهداف المعلنة.

٥. أن تتفق مع الالتزامات.

### ٣. الانتقاص من الالتزامات بحقوق الإنسان أثناء حالة

#### الطوارئ

يجيز القانون الدولي لحقوق الإنسان للدول الانتقاص من بعض التزاماتها في مجال حقوق الإنسان خلال حالة الطوارئ. ويجوز للدولة أن تعلن حالة الطوارئ في ظروف استثنائية عندما تتعرض حياة «الأمة» للتهديد. ويشمل ذلك التهديدات الخطيرة والشبكة للأمن المادي للسكان و / أو لعمل المؤسسات الديمقراطية. ويرجع قرار إعلان حالة الطوارئ وانتقاص حقوق معينة إلى السلطة التنفيذية. ولا تشترك أجهزة الاستخبارات في هذه العملية.

وعند إعلان حالة الطوارئ، يجب على الدولة أن تخطر هيئة المعاهدة ذات الصلة وتحديد حقوق الإنسان التي علقتها أو حدت منها. ويجب أن يكون تعليق أو تقييد حقوق معينة أمراً مؤقتاً تتطلبه الضرورة القصوى للتعامل مع حالات الطوارئ ومتناسب مع الخطر الذي تواجهه الدولة. وبالإضافة إلى ذلك، يجب أن يخضع أي تعليق أو تقييد للحقوق لمراجعة القضاء والبرلمان. ولا يسمح للدول بانتقاص أي حق من الحقوق غير القابلة للانتقاص المذكورة أعلاه أو أية حقوق أخرى غير قابلة للانتقاص واردة في معاهدات حقوق الإنسان الإقليمية والدولية. ووفقاً لذلك، لا يمكن استخدام الأحكام الدستورية

الأخرى لحقوق الإنسان. وتعتبر الدول منتهكة لحقوق الإنسان المعنية إذا أخفقت في الامتثال لهذه المتطلبات.

في كثير من الدول، يخول القانون أجهزة الاستخبارات الحد من الحق في الخصوصية من خلال منحهم صلاحيات خاصة لجمع المعلومات من / عن الأفراد أو المجموعات المشتبه في ضلوعهم في أنشطة محددة تهدد الأمن القومي والسلامة العامة وحقوق الإنسان (انظر صفحة ١٨-١٩). تشمل هذه الصلاحيات الخاصة إجراءات مثل مراقبة اتصالات شخص ما دون علمه أو تصوير أنشطته سرا، ومن ثم فإن هذه التدابير تحد بشكل واضح من حق هذا الشخص في الخصوصية. كذلك تخول بعض الدول أجهزة الاستخبارات فيها أداء مهام إنفاذ القانون (انظر صفحة ٢٨). وفي هذا السياق، يكفل لها القانون الوطني القدرة على اعتقال واحتجاز الأشخاص الذين يشتبه في أنهم ارتكبوا جرائم محددة. وهذه الصلاحيات من شأنها الحد من الحق في الحرية وحرية الحركة.

تفرض الدول الديمقراطية ضوابط صارمة على استخدام أجهزة استخباراتها لهذه الصلاحيات من أجل التأكد من

هويات مزيفة لعملائها للسماح لهم بالتوغل في المجموعات المهتدة للأمن القومي.

**وأخيراً،** قد تسمح التشريعات لأجهزة الاستخبارات بتقديم طلبات رسمية إلى جهات حكومية أخرى أو شركات من القطاع الخاص للحصول على معلومات عن الأفراد حتى حال انتهاك ذلك للحق في الخصوصية. على سبيل المثال، قد يسمح لها في بعض الأحيان بطلب سجلات الهاتف الشخصي من موفري خدمات الاتصالات.

### ما هي المعلومات المسموح لأجهزة الاستخبارات بجمعها؟

في المجتمعات الديمقراطية، تنص القوانين الوطنية على المعلومات المسموح لأجهزة الاستخبارات بجمعها. حيث تسمح القوانين لأجهزة الاستخبارات بجمع معلومات عن أنشطة محددة قد تشكل تهديداً للأمن القومي، على النحو المحدد في اختصاصاتها القانونية، وكذا جمع معلومات عن الأفراد والجماعات الضالعة في هذه الأنشطة إذا كانت هذه المعلومات ذات صلة وضرورية لأداء مهامها.

### ما هي المعلومات غير المسموح لأجهزة الاستخبارات بجمعها؟

تحدد قوانين الاستخبارات أنواع المعلومات المسموح لضباط الاستخبارات بجمعها.

فأولاً، تحظر القوانين جمع المعلومات عن الأفراد والأنشطة التي لا تشكل أي تهديد للأمن القومي.

ثانياً، عادة ما تحظر القوانين المعمول بها في المجتمعات الديمقراطية على ضباط الاستخبارات جمع المعلومات ذات الصلة بالأنشطة السياسية والاجتماعية المكفولة بموجب القانون. على سبيل المثال، لا يجوز لأجهزة الاستخبارات جمع معلومات عن أنشطة مشروعة للأحزاب السياسية وأعضائها أو عن المجموعات المشاركة في الاحتجاجات السلمية. ومن هنا نرى أن هذه المحظورات القانونية تضمن حماية حقوق الإنسان وغيرها من القيم الأخرى ذات الأهمية في المجتمعات الديمقراطية مثل حرية تكوين الجمعيات والتجمع.

وأخيراً، عادة ما تحظر القوانين على ضباط الاستخبارات جمع معلومات من شأنها تحقيق مصالح خاصة. على سبيل المثال، يحظر القانون التجسس على الخصوم السياسيين في حزب معين.

الوطنية الخاصة بسلطات الطوارئ لتبرير الإجراءات التي تنتهك القانون الدولي لحقوق الإنسان.

وإذا ما أُعطيت أجهزة الاستخبارات صلاحيات إضافية لتقييد حقوق الإنسان أثناء حالة الطوارئ، فيجب أن تستمر في الامتثال للقانون الدولي والوطني لحقوق الإنسان، ويجب أن تظل أنشطتها تحت رقابة وإشراف السلطة التنفيذية والبرلمان والسلطة القضائية وأية هيئات إشراف قائمة ذات خبرة.

## جمع المعلومات

### كيف تقوم الاستخبارات بجمع المعلومات؟

في المجتمعات الديمقراطية، تقوم أجهزة الاستخبارات بجمع الكثير من المعلومات التي تحتاجها لإنجاز مهامها من مصادر عامة مثل المقالات والتقارير التي تصدرها المنظمات الحكومية وغير الحكومية والمنشورات الأكاديمية. ويجوز لأجهزة الاستخبارات أيضاً جمع المعلومات من أشخاص لديهم هذه المعلومات أو يمكنهم الحصول على معلومات ذات صلة. فعلى سبيل المثال، قد يعمل أعضاء من المجموعات المهتدة للأمن القومي كمخبرين لدى أجهزة الاستخبارات من خلال تزويدها بالمعلومات سرا. إضافة إلى ما تقدم، يمكن لأجهزة الاستخبارات استخدام أشخاص بأسماء مستعارة أو هويات مزيفة للتوغل في مثل هذه المنظمات وتزويد الأجهزة بمعلومات عن أنشطتها.

ومع ذلك، فبطبيعة الحال لا يفصح الأفراد والجماعات التي تخطط لتهديد الأمن القومي عن نواياهم. وبالتالي، تحتاج المجتمعات الديمقراطية إلى تشريع يمكن أجهزة الاستخبارات من جمع المعلومات التي لا يمكن العثور عليها في المجال العام. وهكذا، تكفل التشريعات صلاحيات خاصة لأجهزة الاستخبارات لا تتوفر عادة لغيرهم من أفراد المجتمع. وتقع هذه الصلاحيات في أربعة مجالات رئيسية.

**أولاً،** قد تتيح التشريعات لأجهزة الاستخبارات مراقبة وسائل الاتصالات الشفهية والإلكترونية والورقية للأفراد دون موافقتهم، وقد تتطلب هذه الأنشطة وسائل تقنية متطورة ومتقدمة.

**ثانياً،** قد تسمح التشريعات لأجهزة الاستخبارات بتصوير الأفراد وممتلكاتهم سرا عن طريق الفيديو والصور الفوتوغرافية دون موافقتهم.

**ثالثاً،** قد تسمح التشريعات لأجهزة الاستخبارات استخدام

- المسموح وغير المسموح لهم بممارسة التحقيق
  - المعلومات المسموح وغير المسموح بجمعها
  - التدابير المسموح باستخدامها لجمع المعلومات
  - متى يجوز أو يحظر استخدام أجهزة الاستخبارات لصلاحياتها الخاصة
  - مدة استخدام هذه الصلاحيات الخاصة
- تتحكم المجتمعات الديمقراطية في استخدام أجهزة الاستخبارات لصلاحياتها الخاصة من خلال المنظمات والعمليات المنشئة لغرض التصريح ومراقبة وتقييم استخدام هذه الصلاحيات الخاصة.

### من الذي يجيز استخدام الصلاحيات الخاصة؟

في المجتمعات الديمقراطية يعتبر استخدام الصلاحيات الخاصة بمثابة الاستثناء وليس القاعدة حيث تفرض المجتمعات الديمقراطية ضوابط صارمة على استخدام هذه الصلاحيات من أجل تقليل المخاطر التي تصاحب استخدامها. ولهذا السبب، يتعين على أجهزة الاستخبارات متى أرادت استخدام صلاحياتها الخاصة أن تطلب تصريحاً من جهة خارجية معنية بهذا الأمر. (انظر مربع ٣ لمزيد من التفاصيل عن هذه العملية في كندا). على أن يكون هذا التصريح مصحوباً بالمبررات الموجبة لاستخدام هذه الصلاحيات. وبدورها تتأكد الجهة المصدرة للتصريح من أن هذا التصريح يتفق مع أحكام القانون.

عادة، ما يكون عضو في السلطة التنفيذية، مثل الوزير المسؤول عن أجهزة الاستخبارات أو إحدى المحاكم هي المسؤولة عن التصريح باستخدام الصلاحيات الخاصة. ومع ذلك، فإن المحكمة هي على الأرجح الجهة المنوط بها مراقبة الحالات التي تنطوي على عمليات تدخل كبيرة في حياة الأفراد، مثل التفتيش ومصادرة الممتلكات ورصد الاتصالات. وفي هذه الحالة تكون المحاكم مستقلة تماماً عن كل أجهزة الاستخبارات والسلطة التنفيذية وتكون في وضع جيد للقيام بتحليل موضوعي لطلبات استخدام الصلاحيات الخاصة.

تطالب بعض الدول السلطتين التنفيذية والقضائية بتولي مسؤولية إصدار التصاريح في استخدام أجهزة الاستخبارات للصلاحيات الخاصة. (انظر على سبيل المثال النموذج الكندي الموضح في مربع ٣). ومن شأن هذه الطريقة إضفاء ضمانة أخرى للتأكد من أن استخدامات الصلاحيات قانونية وضرورية وتستحق المتابعة في ضوء المخاطر التي تنطوي عليها.

### لماذا تقيد الدول الديمقراطية جمع المعلومات من مهنة معينة؟

قد يكون لدى العاملين في بعض المهن مثل الصحفيين والبرلمانيين والمحامين ورجال الدين والأطباء معلومات ذات أهمية لأجهزة الاستخبارات، ومع ذلك، فقد تبنت كثير من المجتمعات الديمقراطية قوانين وتدابير من شأنها تقييد أو منع أجهزة الاستخبارات من جمع معلومات من أو عن أفراد يتقلدون مثل هذه المهن. على سبيل المثال، قد يحظر القانون جمع معلومات حول هؤلاء الأفراد ما لم تكن أجهزة الاستخبارات قد تثبتت من ضلوعهم بشكل مباشر في الأنشطة التي تشكل تهديداً خطيراً للأمن القومي. بالإضافة إلى ذلك، تطبق المجتمعات الديمقراطية ضوابط خاصة لجمع المعلومات عن العاملين في مهنة معينة. والجدير بالذكر أن أجهزة الاستخبارات في بعض الدول تحتاج إلى الحصول على موافقة من رئيس البرلمان قبل التحقيق مع البرلمانين.

إن رغبة المجتمعات الديمقراطية في تقييد جمع المعلومات في بعض المهن، يهدف في المقام الأول إلى حماية الخدمات التي يقدمها القائمون على هذه المهن للسكان. على سبيل المثال، يساعد المحامون المعتقلين على ممارسة حقوقهم في الحرية والمحكمة العادلة، ومن ثم فإذا قامت أجهزة الاستخبارات بمراقبة الاتصالات بين المحامين والمعتقلين فهي بذلك تنتهك حق المعتقل في التواصل سرا مع محاميه. ولنضرب مثالا آخر بالصحفيين، حيث يقومون بالتحقيق في القضايا التي تهم الرأي العام ويعتمدون على الاتصالات السرية لكتابة تحقيقاتهم. وهو دور رقابي أساسي على أنشطة الوكالات الحكومية بغية الكشف عن المخالفات، ومن ثم فإذا قامت أجهزة الاستخبارات بمراقبة اتصالات الصحفيين فقد تعرض هذا الدور الحيوي للإعلام للخطر.

### كيف يحكم المجتمع الديمقراطي استخدام الصلاحيات الخاصة؟

تسن الدول تشريعات لمنح أجهزة الاستخبارات صلاحيات خاصة لجمع المعلومات حول التهديدات التي يتعرض لها الأمن القومي. وهذه الصلاحيات الخاصة هي بمثابة تدابير ليست متاحة قانوناً للوكالات الحكومية الأخرى (باستثناء بعض هيئات الشرطة) أو أفراد من السكان (انظر صفحة ١٨).

تحدد المجتمعات الديمقراطية وتقيّد استخدام أجهزة الاستخبارات لصلاحياتها الخاصة من خلال التشريعات واللوائح التي تحدد:

تقدم أجهزة الاستخبارات تقارير منتظمة إلى السلطة التنفيذية و / أو جهة الرقابة المعنية بشأن ما تحرزه من تقدم خلال العملية، كما تقدم ملخصات عن المعلومات التي تم جمعها والتقدم المحرز والمشاكل التي واجهتها. وتسمح هذه التقارير للمشرفين بتقييم ما إذا كان استخدام الصلاحيات الخاصة قانوني وضروري لأجهزة الاستخبارات حتى تتمكن من أداء مهامها. ويجوز للسلطة التنفيذية و / أو جهة رقابة معينة إنهاء استخدام الصلاحيات الخاصة إذا أخفق جهاز الاستخبارات في الامتثال لأحد أو كافة الضوابط القانونية المتعلقة باستخدام الصلاحيات الخاصة، أو إذا ما قررت جهة الرقابة أنه لم يعد هناك حاجة لاستخدام هذه الصلاحيات.

وأخيراً، تجري جهات الرقابة مراجعات لاستخدام الصلاحيات الخاصة فور الانتهاء منها. وفي بعض الدول، يمكن لجهات الرقابة إصدار أوامر لأجهزة الاستخبارات لحذف المعلومات التي تم جمعها بطرق غير مشروعة. كذلك تراجع جهات الرقابة الخارجية استخدامات الصلاحيات الخاصة لتحديد الاتجاهات التي يمكن أن تساعد الحكومة وأجهزة الاستخبارات في معالجة مشاكل معينة.

### استخدام وإدارة البيانات الشخصية

#### ما هي البيانات الشخصية؟

البيانات الشخصية هي المعلومات الخاصة بشخص معين. ويشمل ذلك حقائق مثل تفاصيل الاتصال بالشخص أو تاريخ الميلاد ورقم جواز السفر والتأمين الاجتماعي. كذلك تشمل البيانات الشخصية المعلومات الأكثر تفصيلاً عن حياة الفرد الخاصة مثل سجلات الصحة أو العمل والمعتقدات الدينية أو الآراء السياسية وتفاصيل عضوية الأحزاب السياسية والنقابات وتفاصيل حول العلاقات مع الشركاء والأصدقاء.

قد تحتاج أجهزة الاستخبارات لجمع البيانات الشخصية للأفراد لتحديد التهديدات المحتملة للأمن القومي.

### كيف تحصل أجهزة الاستخبارات على البيانات الشخصية؟

تحصل أجهزة الاستخبارات على البيانات الشخصية من خلال خمسة طرق رئيسية. أولاً، تقوم أجهزة الاستخبارات بجمع البيانات الشخصية من مصادر عامة أو معلنه. ثانياً، تحصل عليها من خلال استخدام صلاحيات خاصة، مثل

#### كيف تصرح الدولة باستخدام الصلاحيات الخاصة؟

تختلف عملية التصريح باستخدام الصلاحيات الخاصة من دولة إلى أخرى وغالباً ما تعتمد على نوعية الصلاحيات الخاصة التي تنشأ أجهزة الاستخبارات استخدامها. ومع ذلك، فإن القوانين تتطلب عادة اتخاذ الخطوات الثلاثة التالية قبل التصريح لأجهزة الاستخبارات باستخدام الصلاحيات الخاصة. (انظر مربع ٣).

**أولاً،** أن يتقدم عضو معين في أجهزة الاستخبارات بطلب كتابي لاستخدام صلاحية خاصة، والذي عادة ما يشمل:

- وصف النشاط والأفراد و / أو المجموعات المحددة التي تريد أجهزة الاستخبارات التحقيق معها
- توضيح الجهود السابقة لأجهزة الاستخبارات في جمع المعلومات وما الذي حققته هذه الجهود
- الطريقة الخاصة التي ترغب الأجهزة في استخدامها وما الذي ستفعله تحديداً مثل «مراقبة المكالمات على خط هاتف معين»
- تبرير حتمية استخدام الصلاحيات الخاصة ومدى فائدتها في التحقيق.

**ثانياً،** قيام جهة التصريح بفحص الطلب وتحديد ما إذا كان:

- الاستخدام المقترح للصلاحيات الخاصة يتوافق مع جميع القوانين ذات الصلة
- هذا الاستخدام ضروري ومفيد
- هذا الاستخدام يتناسب مع مستوى التهديد الذي يشكله النشاط قيد التحقيق.

**ثالثاً،** إصدار جهة التصريح أمراً يوضح التدابير المحددة المصرح بها وإلى متى يمكن استخدام هذه التدابير.

يتم توثيق عملية الطلب والتصريح المذكورة أعلاه حتى تتمكن أجهزة الاستخبارات وجهات الرقابة من تقييم القرارات في وقت لاحق.

### كيف تشرف المجتمعات الديمقراطية على استخدام الصلاحيات الخاصة؟

في المجتمعات الديمقراطية، تشرف السلطة التنفيذية و / أو جهة الرقابة المعنية على استخدام أجهزة الاستخبارات للصلاحيات الخاصة من خلال رصد العمليات الجارية ومراجعة العمليات التي تمت.

يحدد قانون جهاز الاستخبارات الأمنية الكندي خطوات لطلب وإصدار أوامر لأجهزة الاستخبارات لاستخدام صلاحيات خاصة. ويتعين موافقة مسؤول السلطة التنفيذية وأحد القضاة على أي طلب لاستخدام الصلاحيات الخاصة.

### طلب الحصول على أمر

القسم ٢١

١. عندما يعتقد المدير أو أي موظف يعينه الوزير لهذا الغرض، بناء على أسباب معقولة، أن هناك حاجة بموجب هذا القسم لأمر يمكن جهاز الاستخبارات من التحقيق في تهديد لأمن كندا أو لأداء واجباته ومهامه بموجب القسم ٦١، يجوز للمدير أو الموظف بعد الحصول على موافقة الوزير، التقدم بطلب وفقا للفقرة الفرعية (٢) إلى أحد القضاة لاستصدار أمر بموجب هذا القسم.

### المسائل التي ينبغي تحديدها في الطلب

٢. كون الطلب المقدم للقاضي بموجب الفقرة الفرعية (١) طلبا كتابيا مصحوبا بشهادة خطية من صاحب الطلب توضح المسائل التالية:

- أ. الحقائق المعتمد عليها لتبرير اعتقادهم، بناء على أسباب معقولة، بموجب هذا القسم بالحاجة إلى أمر لتمكين جهاز الاستخبارات للتحقيق في تهديد لأمن كندا أو لأداء واجباته ومهامه بموجب القسم ٦١؛
- ب. أن إجراءات التحقيق الأخرى قد جربت وفشلت، أو تبرير أنه من غير المرجح نجاحها، وأن الحاجة الملحة لمثل هذا الأمر ترجع إلى أنه سيكون من غير العملي الاقتصار في إجراء التحقيق على استخدام إجراءات تحقيق أخرى أو لحقيقة أن عدم وجود أمر بموجب هذا القسم من المحتمل أن يعوق الحصول على المعلومات ذات الأهمية بالنسبة للتهديد لأمن كندا أو أداء الواجبات والمهام في إطار القسم ٦١ المشار إليها في الفقرة (أ).
- ج. نوع الاتصالات المقترح اعتراضها ونوع المعلومات أو السجلات أو الأشياء المقترح الحصول عليها وكذا الصلاحيات المشار إليها في الفقرات (٣) (أ) إلى (ج): المقترح ممارستها لهذا الغرض.
- د. هوية الشخص، إذا كانت معروفة، المقترح اعتراض اتصالاته أو من يحوز المعلومات أو السجلات أو الوثائق أو الأشياء المقترح الحصول عليها.
- هـ. الأشخاص أو فئات الأشخاص المقترح توجيه الأمر إليهم.
- و. وصفا عاما للمكان المقترح تنفيذ الأمر فيه، إذا كان من الممكن توفير وصف عام له.
- ز. المدة - لا تزيد على ستين يوما أو سنة واحدة حسب الحالة - المطلوب سريان الأمر خلالها والمعمول بها بموجب الفقرة الفرعية (٥).
- ح. أي طلب سبق تقديمه له علاقة بالشخص المحدد في الشهادة الخطية وفقا للفقرة (د) وتاريخ تقديم الطلب واسم القاضي الذي تم رفع الطلب إليه وقرار القاضي في هذا الشأن.

### إصدار الأمر

٣. بصرف النظر عن أي قانون آخر ودون المساس بقانون الإحصاء، متى رأى القاضي المرفوع له الطلب بموجب الفقرة الفرعية (١) استيفاء الطلب للمسائل المشار إليها في الفقرتين (٢) (أ) و(ب) المنصوص عليها في الشهادة الخطية المصاحبة للطلب، يصدر القاضي أمرا يصرح للأشخاص الموجه إليهم الأمر باعتراض أي رسالة أو الحصول على أية معلومات أو سجلات أو وثائق أو أشياء، ولهذا الغرض.

- أ. الدخول إلى أي مكان أو فتح أو الحصول على أي شيء؛
- ب. تفتيش أو إزالة أو إعادة، أو فحص أو أخذ مقتطفات من أو عمل نسخ من سجل أو بأي طريقة أخرى الحصول على معلومات أو سجلات أو وثائق أو أشياء، أو
- ج. تثبيت وصيانة أو إزالة أي شيء.

**المسائل التي ينبغي تحديدها في الأمر**

٤. يجب تحديد ما يلي في الأمر الصادر بموجب الفقرة الفرعية (٣)
  - أ. نوع الاتصالات المصرح باعتراضها ونوع المعلومات والسجلات والوثائق أو الأشياء المصرح بالحصول عليها والصلاحيات المشار إليها في الفقرات (٣) (١) إلى (ج) المصرح بممارستها لهذا الغرض.
  - ب. هوية الشخص، إذا كانت معروفة، المقرر اعتراض اتصالاته أو من يحوز المعلومات أو السجلات أو الوثائق أو الأشياء المقرر الحصول عليها.
  - ج. الأشخاص أو فئات الأشخاص الموجه إليهم الأمر.
  - د. وصفا عاما للمكان المقرر تنفيذ الأمر فيه، إذا كان من الممكن توفير وصف عام له.
  - هـ. مدة سريان الأمر.
  - و. الأحكام والشروط التي يرى القاضي أنها تصب في المصلحة العامة.

**لماذا تقيد المجتمعات الديمقراطية استخدام المعلومات الشخصية؟**

تقيد المجتمعات الديمقراطية استخدام البيانات الشخصية من قبل أجهزة الاستخبارات لثلاثة أسباب رئيسية. أولاً، تقيد المجتمعات الديمقراطية استخدام البيانات الشخصية بسبب المخاطر المتأصلة التي قد يتعرض لها الأفراد نتيجة الكشف عن البيانات الشخصية الخاصة بهم، حيث إن البيانات الشخصية تحتوي على معلومات عن أكثر الجوانب خصوصية من حياة الفرد، بما في ذلك السجلات الطبية والمعتقدات الدينية والمواقف السياسية والعلاقات الشخصية. إضافة إلى ذلك فإن كشف النقاب عن هذه المعلومات يعرض فرص حصولهم على عمل والعلاقات الشخصية والمهنية والسلامة الشخصية للخطر.

ثانياً، هناك خطورة محتملة من أن أجهزة الاستخبارات و / أو جهات أخرى ممن يمكنهم الوصول بموجب القانون إلى بيانات الفرد الشخصية قد تستخدم هذه البيانات في أغراض غير قانونية. على سبيل المثال، قد تميل أجهزة الاستخبارات و / أو السلطة التنفيذية إلى استخدام البيانات الشخصية لتشويه سمعة المعارضين السياسيين أو ابتزازهم. ولذلك تحتاج الحكومات الديمقراطية لتقييد استخدام البيانات الشخصية من خلال التشريعات.

وأخيراً، فإن الأفراد عادة ما يجهلون نوعية البيانات الشخصية التي تحتفظ بها الاستخبارات عنهم. وبالتالي، فإنها قد لا تتمكن من الاعتراض على استخدام أجهزة الاستخبارات للبيانات الشخصية الخاصة بهم أو الوقوف على دقة هذه البيانات. ولذلك، فمن الضروري أن تسن القوانين قواعد واضحة لاستخدام البيانات الشخصية وأن تقوم جهات الرقابة بمتابعة الامتثال لهذه القواعد.

مراقبة الاتصالات سرا (انظر صفحة ١٨). ثالثاً، قد تقوم الأجهزة بطلب المعلومات والبيانات الشخصية عن شخص معين من الجهات الحكومية الداخلية مثل إدارات الهجرة. رابعاً، قد يقدم المخبرون معلومات شخصية إلى أجهزة الاستخبارات. وأخيراً، يمكن لأجهزة الاستخبارات الحصول على بيانات شخصية عن أفراد معينين من الحكومات الأجنبية و / أو أجهزة الاستخبارات التابعة لها.

**كيف تستخدم أجهزة الاستخبارات وحكوماتها البيانات الشخصية؟**

تحتفظ أجهزة الاستخبارات بقدر كبير من البيانات الشخصية التي تجمعها في ملفات إلكترونية أو ورقية ليسهل الوصول إليها. فوفاً، تقوم باستخدام هذه الملفات لدعم التحقيقات الجارية والمستقبلية التي تهدد الأمن القومي، فضلاً عن إمكانية استخدامها للبيانات الشخصية لتقييم الأفراد المتقدمين بطلبات للحصول على تصاريح أمنية حكومية.

ثانياً، تتبادل أجهزة الاستخبارات البيانات الشخصية مع الوكالات والمسؤولين الحكوميين مثل سلطات إنفاذ القانون والمدعين العموم. وتستخدم الحكومات البيانات الشخصية بصورة متزايدة من أجهزة الاستخبارات لدعم اتخاذ إجراءات قانونية ضد أفراد معينين، حيث يستخدمون البيانات الشخصية في عمليات مكافحة الإرهاب لتبرير حظر السفر ورفض التأشيرات ومصادرة الأصول وتقييد حركة الفرد والاتصالات مع الآخرين.

وفي ظروف استثنائية، يجوز السماح لأجهزة الاستخبارات بتبادل البيانات الشخصية مع الحكومات الأجنبية ووكالاتها. مزيد من المعلومات يرجى الرجوع إلى قسم التعاون الدولي في مجال الاستخبارات في هذا الدليل.

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

٤ للوقوف على مثال للتشريعات بشأن استخدام البيانات الشخصية من قبل أجهزة الاستخبارات في ألمانيا). وعلى الرغم من أن هذه الضوابط معقدة؛ إلا أن المقام لا يتسع هنا سوى لمناقشة ثلاثة أنواع فقط من الضوابط القانونية.

**أولاً،** تحدد القوانين الوطنية أنواع البيانات الشخصية التي يجوز لأجهزة الاستخبارات استخدامها. على سبيل المثال، تسمح قوانين أجهزة الاستخبارات استخدام البيانات الشخصية للأفراد المشاركين في الأنشطة التي تهدد الأمن القومي، كعضويتهم في منظمة إرهابية مثلاً. وتتطلب القوانين أن يرتبط استخدام البيانات الشخصية بسلوك الفرد، أي بخلوعه في الأنشطة التي تهدد الأمن القومي. وتحظر

## ما هي الضوابط القانونية التي تنطبق على استخدام البيانات الشخصية؟

تحتاج أجهزة الاستخبارات إلى جمع بعض البيانات الشخصية والاستفادة منها من أجل أداء مهامها. وعلى وجه الخصوص، لا بد أن تكون قادرة على التعرف على أفراد معينين وجمع المعلومات عن سلوكهم وأنشطتهم من أجل تحديد التهديدات المحتملة على الأمن القومي. وبوضع هذا في الاعتبار، تسن الدول قوانين تسمح لأجهزة الاستخبارات باستخدام بيانات شخصية معينة دون موافقة الأشخاص المعنيين. ومن خلال التشريعات، تطبق الدول أيضاً ضوابط صارمة لتنظيم استخدام البيانات الشخصية. (انظر مربع

### مربع ٤: لوائح استخدام البيانات الشخصية من قبل المكتب الاتحادي الألماني لحماية الدستور<sup>٧</sup>

يفرض القانون الألماني رقابة صارمة على استخدام البيانات الشخصية من قبل المكتب الاتحادي لحماية الدستور (جهاز الاستخبارات الداخلي الألماني). تمثل المقتطفات التالية من قانونين ألمانيين أمثلة على الممارسات الجيدة في مجال جمع البيانات الشخصية والاحتفاظ بها وحذفها. حيث يتم مراقبة جميع هذه الأنشطة بواسطة لجنة العشر G10، وهي هيئة إشرافية مستقلة لها حق الوصول إلى جميع المعلومات التي تحتفظ بها أجهزة الاستخبارات.

### أسباب جواز استخدام البيانات الشخصية

• لأداء مهامه، يجوز للمكتب الاتحادي لحماية الدستور تخزين وتعديل واستخدام البيانات الشخصية في الحالات التالية:

١. وجود مؤشرات فعلية لجهود أو أنشطة وفقاً للمادة ٣، الفقرة ١ (وتشمل هذه الأنشطة ما يلي: الجهود الموجهة ضد النظام الأساسي الديمقراطي الحر، وجود أو أمن الاتحاد أو إحدى الدول، أو السعي بصورة غير قانونية إلى إعاقة الهيئات الدستورية للاتحاد أو إحدى دوله من أداء واجباتها)

٢. أن يكون ضرورياً من أجل التحقيق وتحليل الجهود أو الأنشطة وفقاً للمادة ٣، الفقرة ١

٣. أن يتخذ المكتب الاتحادي لحماية الدستور إجراءات في إطار القسم ٣، الفقرة الفرعية ٢ (وهي، ضد الأنشطة التي تهدد الأمن أو أنشطة الاستخبارات التي يقومون بها نيابة عن قوة أجنبية)

- لوائح بشأن التخزين وتصحيح وحذف البيانات الشخصية التي يحتفظ بها المكتب الاتحادي لحماية الدستور.
- يقيد المكتب الاتحادي لحماية الدستور مدة تخزين (البيانات الشخصية) بالقدر اللازم لأداء مهامه.
- يتم تصحيح البيانات الشخصية غير الصحيحة في الملفات المخزنة من قبل المكتب الاتحادي لحماية الدستور.
- عند التعامل مع حالات معينة، يفحص المكتب الاتحادي لحماية الدستور ضمن فترات زمنية معينة، بعد مرور خمس سنوات على أقصى تقدير، ما إذا كان ينبغي تصحيح أو حذف البيانات الشخصية المخزنة
- يتعين حذف البيانات الشخصية المخزنة في الملفات من قبل المكتب الاتحادي لحماية الدستور إذا كان قد تم تخزينها بشكل غير مقبول أو لم تعد هناك حاجة لها في إنجاز مهامه. ولا يجوز حذف البيانات إذا كان هناك سبب للاعتقاد بأن هذا الحذف من شأنه أن يخل بالمصالح المشروعة لصاحب البيانات. وفي هذه الحالة، يتعين حظر البيانات وعدم تناقلها إلا بموافقة صاحب البيانات.

### الإشراف

- تمتد الصلاحيات الإشرافية للجنة العشر (G10) لتنطبق على كامل نطاق جمع ومعالجة واستخدام البيانات الشخصية التي تم الحصول عليها وفقاً لهذا القانون من قبل أجهزة الاستخبارات التابعة للاتحاد.

بعض الأفراد. ويتعين في بعض الدول حصول أجهزة الاستخبارات على موافقة جهات الرقابة قبل إنشاء ملف عن أحد الأفراد.

تقوم هيئات الرقابة أيضا بالتحقق من ملفات أجهزة الاستخبارات للتأكد من أنها تتعامل مع البيانات الشخصية وفقا للقوانين واللوائح. ويجوز لها مراجعة الملفات بمبادرة منها أو استجابة لطلبات أفراد للاستعلام عن ملفاتهم. وفي بعض الدول، ينص القانون على مطالبة أجهزة الاستخبارات في بعض الأحيان بإبلاغ جهات الرقابة حال تبادل البيانات الشخصية مع مؤسسات أخرى، أو عند حذف معلومات من ملفات البيانات الخاصة بهم. وأخيرا، تقوم جهات الرقابة في كثير من الدول بمراجعة طريقة تعامل الاستخبارات مع طلبات الأفراد للوصول إلى بياناتهم الشخصية التي تحتفظ بها أجهزة الاستخبارات. (انظر مربع ٥).

### هل يمكن للأفراد الوصول إلى بياناتهم الشخصية؟

في الدول الديمقراطية، يحق لأفراد الجمهور التقدم بطلبات للوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات. (انظر مربع ٥ للوقوف على مثال عن كيفية القيام بهذه العملية في ألمانيا). وحتى يمكنهم الوصول إلى بياناتهم الشخصية، يتعين عليهم تقديم طلب مباشرة إلى أجهزة الاستخبارات أو من خلال الموظف المسؤول في الجهة التنفيذية عن أجهزة الاستخبارات. وبعد عرض البيانات الشخصية، يجوز لأفراد الجمهور تقديم طلبات لحذف و / أو تغيير البيانات.

وفي بعض الحالات، تسمح القوانين واللوائح لأجهزة الاستخبارات برفض الطلبات المقدمة من الأفراد للوصول إلى البيانات الشخصية. فعلى سبيل المثال، يمكن رفض طلبات من أجل الحفاظ على سرية تحقيقات جارية أو لضمان السلامة العامة أو لحماية مصالح الأمن القومي. وعادة لا يتعين على أجهزة الاستخبارات إطلاع الأفراد على أسباب رفض الطلبات. ومع ذلك، يجوز لجهات الإشراف الخارجية مراجعة الطعن في قرارات أجهزة الاستخبارات الخاصة برفض الطلبات.

وقد يجوز للأفراد مطالبة هذه الجهات بمراجعة الحالات الخاصة بهم، وهو ما يساعد في ضمان أن قرارات رفض الوصول إلى بيانات شخصي تعتبر ضرورة لا مندوحة عنها.

المجتمعات الديمقراطية على أجهزة الاستخبارات استخدام البيانات الشخصية على أساس الخصائص الشخصية مثل العرق أو الدين أو الجنس. وبالإضافة إلى ذلك، تحظر قوانين أجهزة الاستخبارات استخدام أجزاء من بيانات فرد لا صلة لها بتهديد الأمن القومي، مثل السجلات الطبية، حتى لو كان هذا الفرد متورطا في أنشطة تهدد الأمن الوطني.

**ثانياً،** تضع القوانين حدودا على الاحتفاظ بالبيانات الشخصية. ويمكن لأجهزة الاستخبارات الاحتفاظ بالبيانات الشخصية فقط إذا كان ذلك ضروريا لتحديد وتحليل تهديد محدد للأمن القومي. وتتطلب القوانين من أجهزة الاستخبارات مراجعة ملفاتهم بشكل منتظم من أجل تحديث ملفات البيانات الشخصية. وفي العديد من المجتمعات الديمقراطية تتطلب القوانين الوطنية من أجهزة الاستخبارات حذف البيانات الشخصية التي لم تعد ذات صلة أو غير ضرورية، مثل البيانات الشخصية للأفراد الذين لا يشكلون تهديدا للأمن القومي.

**ثالثاً،** ينظم القانون عملية الوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات. ويجوز لبعض الموظفين فقط في أجهزة الاستخبارات الوصول إلى ملفات البيانات الشخصية. ويتطلب القانون أيضا توثيق جميع عمليات الوصول على ملفات البيانات الشخصية من قبل هؤلاء الأفراد. وتهدف هذه الضوابط إلى منع إساءة استخدام البيانات الشخصية.

**رابعاً،** يقيد القانون إفصاح أجهزة الاستخبارات عن البيانات الشخصية للاستخدام من قبل وكالات حكومية أخرى. ويقتصر تبادلهم للبيانات الشخصية مع هيئات حكومية مصرحة لها بذلك ممن تحتاج هذه المعلومات لتنفيذ مهامها. ويتم وضع قيود صارمة على طريقة استخدام هذه الهيئات للبيانات الشخصية المتبادلة معهم من قبل أجهزة الاستخبارات.

### من الذي يشرف على استخدام البيانات الشخصية وما هي مهمته؟

تشرف جهات الرقابة الخارجية على استخدام أجهزة الاستخبارات للبيانات الشخصية للتأكد من استخدام البيانات وفقا للقانون. وتشمل هذه الجهات جهات الرقابة البرلمانية وذات الخبرة، فضلا عن المؤسسات المعنية بحماية البيانات. (انظر صفحة ٣٤-٤٣).

وتقوم هذه الجهات بمراجعة قرارات أجهزة الاستخبارات بشأن الاحتفاظ بالبيانات الشخصية وإنشاء ملفات عن

ثانياً، تقوم بعض أجهزة الاستخبارات بعمليات مشتركة مع شركائها الأجانب، على سبيل المثال يمكن لعملاء من مختلف أجهزة الاستخبارات التعاون سويًا لجمع المعلومات. أو قد يقوم جهاز الاستخبارات في بلد ما بمشاركة بنيتها التحتية مع أجهزة استخبارات أجنبية.

**ثالثاً،** قد ينطوي التعاون الدولي في مجال الاستخبارات على تبادل المعارف والخبرات. على سبيل المثال، يمكن لأجهزة الاستخبارات تدريب نظرائهم الأجانب أو إرسال ضباط الاستخبارات لدعم عمل أجهزة الاستخبارات الأجنبية.

## التعاون الدولي في مجال الاستخبارات

### ما هو التعاون الدولي في مجال الاستخبارات؟

يصف مصطلح «التعاون الدولي في مجال الاستخبارات» طرق عمل أجهزة الاستخبارات والأمن في بلدين أو أكثر مع بعضهم البعض. جدير بالذكر أن أجهزة الاستخبارات تتعاون مع الكيانات الأجنبية من خلال ثلاث طرق رئيسية. **الطريقة الأولى** وهي الأكثر شيوعاً تبادل أجهزة الاستخبارات للمعلومات مع نظرائهم الأجانب. ويجوز للأجهزة تبادل البيانات الخام أو تقديم تحليلات للمعلومات لأجهزة الاستخبارات الأجنبية.

### مربع ٥: القانون الألماني بشأن إمكانية الوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات<sup>١</sup>

- يكفل القانون الألماني للجمهور حقاً عاماً في الوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات من خلال التقدم بطلبات مباشرة إلى أجهزة الاستخبارات. توضح المقتطفات التالية كيفية سير هذه العملية.
- التقدم بطلب للوصول إلى البيانات الشخصية التي تحتفظ بها أجهزة الاستخبارات.
- يزود المكتب الاتحادي لحماية الدستور صاحب البيانات مجاناً، عند طلبه / طلبها، بالمعلومات الخاصة بالبيانات الشخصية المخزنة عنه / عنها، إذا أشار المتقدم إلى مسائل الملموسة وأثبت أن له مصلحة خاصة في المعلومات محل الطلب.

### أسباب رفض الوصول إلى البيانات الشخصية

- لا يجوز تقديم المعلومات في الحالات التالية:
  ١. إمكانية المساس بأداء المهام بشكل سليم
  ٢. إمكانية تعريض المصادر للخطر، أو إذا خشي المكتب الاتحادي لحماية الدستور إمكانية الكشف عنه أو عنه طريقة عمله،
  ٣. إمكانية الإضرار بالسلامة العامة أو يضر بالاتحاد أو دولة فيه
  ٤. حتمية الإبقاء على سرية البيانات أو الحقائق المخزنة وفقاً لأحكام قانونية أو بحكم طبيعتها، ولا سيما إذا كانت متعلقة بمصلحة طرف ثالث.
- يتعين اتخاذ القرار من قبل رئيس المكتب الاتحادي لحماية الدستور أو من قبل موظف مأذون له بذلك صراحة.
- لا يتضمن الالتزام بتقديم المعلومات عن أصل البيانات والمستفيدين من البيانات المنقولة.
- لا يتعين ذكر أسباب رفض تقديم المعلومات إذا كان ذكرها قد يكشف عن الغرض من رفض تقديم المعلومات. ويتعين في هذه الحالة إدراج أسباب الرفض في السجلات.

### الحق في الاستئناف

- في حالة رفض تقديم معلومات، يتعين إخطار صاحب البيانات بالأساس القانوني لسبب الرفض وحقائق إمكانية استئناف ذلك أمام المفوض الاتحادي لحماية البيانات والذي ينبغي تزويده بهذه المعلومات متى طلب ذلك ما لم تقرر وزارة الداخلية الاتحادية في قضية معينة أن هذا سيشكل خطراً على أمن الاتحاد أو دولة فيه.

محلية انطوت على انتهاك لحقوق الإنسان، فيمكن اعتبارهم متواطئين.

**ثالثاً،** قد ترغب بعض أجهزة الاستخبارات في التعاون مع شركاء أجنبى لمنع سلطات هؤلاء الشركاء من مراقبة أنشطتهم. فقد ترغب أجهزة الاستخبارات تحديداً تجنب الضوابط القانونية والإشرافية التي قد تستخدمها هذه السلطات لمساءلة الأجهزة عن احترامها لحقوق الإنسان إبان استخدامها للصلاحيات الخاصة لجمع المعلومات.

**وأخيراً،** بالإضافة إلى التهديدات التي تكتنف حقوق الإنسان، فإن التعاون الدولي في مجال الاستخبارات قد يضر بسمعة الدولة والعلاقات الخارجية. فعلى سبيل المثال، قد تتعاون أجهزة الاستخبارات مع وكالة استخبارات أجنبية على نحو يتداخل مع السياسة الخارجية لدولهم. ونظراً لهذه المخاطر، تحاول الدول فرض الرقابة قدر الإمكان على أجهزتها الاستخباراتية حيال عملية التعاون الدولي في مجال الاستخبارات.

### كيف تراقب الدول التعاون الدولي في مجال الاستخبارات؟

تنظم القوانين الوطنية التعاون الاستخباراتي مع الحكومات وأجهزة الاستخبارات الأجنبية، حيث تحدد هذه القوانين واللوائح أجهزة الاستخبارات التي يمكن التعاون معها وما هي الطريقة والظروف التي تحكم عملية التعاون مع هذه الجهات وكيف تصرح الحكومة بهذا التعاون وتشرف عليه. (انظر مربع ٦ للإطلاع على كيفية تنظيم عمل أجهزة الاستخبارات في كرواتيا)

في ضوء المخاطر المرتبطة بالتعاون الدولي في مجال الاستخبارات، تطلب القوانين الوطنية أجهزة الاستخبارات الحصول على موافقة من السلطة التنفيذية قبل الدخول في اتفاق مع جهة أجنبية. وبالإضافة إلى ذلك، عادة ما يتعين على السلطة التنفيذية الموافقة على العمليات أو الأنشطة المشتركة التي تنطوي على مشاركة وتبادل المعلومات التي تشكل خطراً. ومن شأن الحصول على موافقة السلطة التنفيذية على التعاون في مجال الاستخبارات الدولية، ولاسيما في الأنشطة الحساسة ضمان أن أجهزة الاستخبارات لا تعمل دون إشراف من قبل الدولة.

### ما هي الضوابط المطبقة على تبادل المعلومات مع أجهزة الاستخبارات الأجنبية؟

يوجد لدى المجتمعات الديمقراطية قوانين وأنظمة لمراقبة

### لماذا تتعاون أجهزة الاستخبارات مع الحكومات وأجهزة الاستخبارات الأجنبية؟

يرجع تعاون أجهزة الاستخبارات مع نظرائها الأجنبى في المقام الأول إلى حقيقة أن هذا التعاون يعطيها مزيد من المعلومات والخبرات، حيث إن أجهزة الاستخبارات في بلد واحد ليست لديها ما يكفي من الموارد أو الخبرات اللازمة لجمع المعلومات حول التهديدات القائمة ذات الصلة في جميع مناطق العالم وبالتالي، فهي بحاجة إلى الاعتماد على وكالات أجنبية. وتتمتع هذه الجهات الأجنبية بالموقع الجغرافي المناسب فضلاً عن معرفتها لبعض المجموعات واللغات والثقافات التي تمكنها من جمع المعلومات اللازمة. وقد تقوم أجهزة الاستخبارات في بلد ما بتقديم معلومات الاستخبارات لنظيراتها الأجنبية في مقابل الحصول على معلومات أو موارد أخرى، كمعدات أو أموال مثلاً. وقد اكتسب هذا التعاون الدولي بين أجهزة الاستخبارات أهمية متزايدة في ضوء تشعب عمل الجماعات التي تهدد أمن الدول وشعوبها عبر الحدود في عدد من الدول.

### ما هي مخاطر التعاون في مجال الاستخبارات؟

ينطوي التعاون بين الحكومات الأجنبية وأجهزة المخابرات على مجموعة متنوعة من المخاطر لجميع الأطراف المعنية. فأولاً، نجد أن هذا التعاون الدولي يشكل مخاطر جسيمة على حقوق الإنسان المحمية بموجب القانون الدولي. جدير بالذكر أن التعاون الاستخباراتي يمثل تهديداً خاصاً على حقوق الإنسان عندما تتبادل أجهزة الاستخبارات البيانات الشخصية مع كيانات أجنبية. فعلى سبيل المثال، قد ينتهي الأمر بأحد أجهزة الاستخبارات التي تلقت بيانات شخصية باستخدام هذه البيانات على نحو ينتهك حقوق الإنسان إذا ما استخدمتها في تحديد الأشخاص واحتجازهم بشكل غير قانوني و / أو إساءة معاملتهم. وعموماً، فإن أجهزة الاستخبارات عادة ما تخبر الكيانات الأجنبية الشريكة بكيفية استخدام البيانات الشخصية المتبادلة، ولكنها مع ذلك لا تملك حق الرقابة الكاملة على كيفية استخدامها.

**ثانياً،** في كثير من الحالات لا تدري أجهزة الاستخبارات كيفية قيام الجهات الخارجية بجمع المعلومات أو ما إذا كان الحصول على هذه المعلومات قد تم بشكل قانوني أم لا. وعلى وجه التحديد، قد لا تدري هذه الأجهزة ما إذا كانت هذه الجهات الخارجية قد لجأت إلى التعذيب أو غيره من الأساليب الأخرى غير المشروعة للحصول على المعلومات. ومع ذلك، فإذا نما إلى علم مسؤولي الاستخبارات أن المعلومات التي تم الحصول عليها من مصادر أجنبية أو

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

وبالإضافة إلى القوانين واللوائح التي تنظم عمل الاستخبارات، يوجد لدى أجهزة الاستخبارات شروطها الخاصة لتبادل المعلومات مع الشركاء الأجانب. ومن بين الأمثلة الأكثر شيوعاً على ذلك هي مبادئ «سيطرة الجهة الأصلية» و«قاعدة الطرف الثالث». هذه القواعد غير الرسمية تنطبق على معظم عمليات تبادل المعلومات الاستخباراتية. ويشير مصطلح «سيطرة الجهة الأصلية» إلى المبدأ القائل بأن جهاز الاستخبارات المانح للمعلومات هو من يضع حدود استخدام هذه المعلومات. أما مصطلح «قاعدة الطرف الثالث» فيعني أن المتلقي للمعلومات غير مسموح له بتبادلها مع وكالة أخرى أو طرف ثالث آخر دون إذن من أجهزة الاستخبارات التي قدمت هذه المعلومات في الأصل. ومن شأن هذه المبادئ المساعدة في الحيلولة دون الكشف عن المعلومات الحساسة.

كذلك ترفق أجهزة الاستخبارات ملاحظات على المعلومات المتبادلة والتي غالباً ما يشار إليها باسم «المحاذير». هذه الملاحظات توضح كيفية استخدام هذه المعلومات المتبادلة. فعلى سبيل المثال، قد يحظر على الوكالات الأجنبية استخدام معلومات معينة كأساس لاعتقال واحتجاز شخص ما.

أجهزة الاستخبارات حال تبادل المعلومات مع أجهزة استخبارات أجنبية. (انظر مربع ٦). هذه القوانين تحدد ومتى وتحت أي ظروف يجوز لأجهزة الاستخبارات تبادل المعلومات مع الهيئات الأجنبية. فعلى سبيل المثال، لا يجوز لأجهزة الاستخبارات طلب معلومات من جهات أجنبية إلا إذا كانت هذه المعلومات لازمة لأداء مهامها. وبالمثل، فإنها لا تعطي معلومات لجهات أجنبية إلا إذا كانت هذه المعلومات لازمة لأداء مهامها هي الأخرى.

وبالإضافة إلى ذلك، فإن القانون يتطلب من أجهزة الاستخبارات التفكير فيما إذا كان تبادل أو عدم تبادل معلومات محددة سوف يكون في مصلحة الدولة أم لا. فعلى سبيل المثال، تتطلب بعض القوانين من أجهزة الاستخبارات التفكير فيما إذا كان تبادل المعلومات مع جهة أجنبية يخدم السياسة الخارجية للدولة أم لا. والأهم من ذلك، أنه يتعين على أجهزة الاستخبارات التفكير في آثار تبادل المعلومات على الأفراد موضوع هذه المعلومات. وتحظر القوانين في المجتمعات الديمقراطية تبادل المعلومات مع الجهات الأجنبية إذا كانت هذه المعلومات من المرجح أن تعرض حياة الأفراد للخطر أو تؤدي إلى انتهاكات أخرى لحقوق الإنسان.

### المربع ٦: اللوائح الكرواتية المتعلقة بالتعاون الاستخباراتي مع كيانات أجنبية<sup>٩</sup>

يرسي قانون نظام الاستخبارات الأمنية لجمهورية كرواتيا الأساس القانوني لأجهزة الاستخبارات الكرواتية للتعاون مع الكيانات الخارجية ويحدد الضوابط التي تنطبق على تبادل البيانات الشخصية مع هذه الكيانات.

#### المادة ٥٩

١. بناء على التزاماتها الدولية، يجوز لوكالات الاستخبارات الأمنية التعاون مع الأجهزة الأمنية والاستخباراتية الأجنبية وغيرها من الأجهزة الأخرى المعنية، من خلال تبادل المعلومات والمعدات، ومن خلال الأنشطة المنفذة بصورة مشتركة في المجالات ذات الصلة، وكذلك من خلال تعليم الموظفين.
٢. يتم الموافقة على تفعيل وتعليق التعاون مع الأجهزة الأجنبية بواسطة مجلس الأمن القومي بناء على توصيات مديري وكالات الاستخبارات الأمنية ورأي مجلس التنسيق بين وكالات الاستخبارات الأمنية.

#### المادة ٦٠

١. يجوز لوكالات الاستخبارات الأمنية أن تتبادل مع الأجهزة الأجنبية المناسبة معلومات عن المواطنين في جمهورية كرواتيا إذا كانت قد حصلت على بيانات ذات صلة تشير أن هذا الشخص يشكل تهديدا للأمن القومي للدولة التي يتم تزويدها بالبيانات، أو تهديدا للقيم التي يحميها القانون الدولي. ولا يجوز تقديم المعلومات إذا كان ذلك مخالفا لمصالح جمهورية كرواتيا، أو إذا كانت حماية مصالح الشخص المعني ذات قيمة أكبر.
٣. لا بد من إدخال البيانات المسلمة في السجلات. وترفق هذه البيانات عن طريق إشعار يشير إلى أنه لا يجوز استخدامها إلا في الغرض المسلمة من أجله، وأن وكالة الاستخبارات الأمنية الموفرة للبيانات تحتفظ بحقوقها في طلب معلومات عن الكيفية التي تم بها استخدام المعلومات المقدمة.

## استخدام أجهزة الاستخبارات لصلاحيات الاعتقال والاحتجاز

### هل من المناسب منح أجهزة الاستخبارات صلاحيات اعتقال واحتجاز الأفراد؟

لا يسمح القانون الوطني في معظم المجتمعات الديمقراطية لأجهزة الاستخبارات باستخدام صلاحيات الاعتقال والاحتجاز. حيث إن هذه الصلاحيات عادة ما يتم إعمالها لدعم تطبيق القانون وليس لمساندة أجهزة الاستخبارات في جمع المعلومات. ومن هنا لا يسمح القانون الدولي لحقوق الإنسان باعتقال و / أو احتجاز الأفراد لغرض جمع المعلومات.

ومع ذلك، فإن بعض الدول الديمقراطية تعطي أجهزة الاستخبارات صلاحيات اعتقال واحتجاز الأشخاص الذين ارتكبوا أو على وشك ارتكاب جرائم تهدد الأمن الوطني. فعلى سبيل المثال، قد يقبضون على أشخاص متورطين في الإعداد لهجمات إرهابية أو نشر أسلحة دمار شامل. وكثيرا ما يتم السماح لأجهزة الاستخبارات في الدول التي ليس لها تنظيم منفصل للاستخبارات وإنما تكون مهام الاستخبارات فيها تابعة للشرطة باستخدام صلاحيات القبض والاحتجاز. وفي ظل مثل هذه النظم غالبا ما يقوم الأفراد المسؤولين عن جمع المعلومات الاستخباراتية بإجراء التحقيقات الجنائية في الأعمال الإرهابية ويضطلعون بمسؤولية اعتقال واحتجاز أشخاص يشتبه في ارتكابهم تلك الجرائم. وفي هذا السياق، قد يتعين أن ينص القانون الوطني على السماح لأجهزة الاستخبارات باستخدام صلاحيات الاعتقال والاحتجاز.

### ما هي المعايير الدولية المطبقة على استخدام صلاحيات الاعتقال والاحتجاز؟

تقوم المجتمعات الديمقراطية التي تسمح لضباط الاستخبارات باعتقال واحتجاز الأفراد بتضمين قانونها الوطني معايير مقبولة دوليا بشأن الاعتقال والاحتجاز. (انظر مربع ٧).

تنطبق هذه المعايير على أجهزة الاستخبارات في الفئات التالية:

- القوانين والأساس المنطقي لاعتقال واحتجاز الأفراد
- معاملة الأفراد قيد الاحتجاز
- الإشراف على عمليات الاعتقال والاحتجاز ومراجعتها.

وتحتفظ أجهزة الاستخبارات بحق مطالبة الجهة الأجنبية بالإفصاح عن الجهات التي قدمت لها المعلومات وعن كيفية استخدامها لهذه المعلومات. ومرة أخرى نجد أن هذه القواعد غير الرسمية تساعد في الحد من إساءة استخدام المعلومات من قبل جهات أجنبية وربما تعزز مزيدا من الاحترام لحقوق الإنسان.

### كيف يتم الإشراف على التعاون الدولي في مجال الاستخبارات؟

في المجتمعات الديمقراطية، تراقب جهات الإشراف الخارجية التعاون الدولي في مجال الاستخبارات للتأكد من أنها تتماشى مع القانون، حيث تقوم بالرقابة على التعاون الاستخباراتي بعدة طرق: أولا، مراجعة اتفاقات الاستخبارات مع الشركاء الأجانب لضمان امتثال هذه الاتفاقات للقانون.

ثانيا، يجب على أجهزة الاستخبارات في بعض الدول إبلاغ جهة الرقابة بشأن تبادل المعلومات مع جهات أجنبية. ومن خلال تراكم معرفة جهة الرقابة بتبادل المعلومات بمرور الوقت، تصبح هذه الجهة قادرة على رصد الأنماط، وإذا لزم الأمر، تقييم علاقات تعاونية وأنشطة معينة مع بعض أجهزة الاستخبارات. ويجوز لهيئات الرقابة أيضا فحص المعلومات التي أرسلتها أجهزة الاستخبارات إلى جهات أجنبية، حيث إن الإطلاع على هذه المعلومات المتبادلة تمكنها من تقييم ما إذا كان قرار إرسال المعلومات ضروريا ومناسبا في ضوء آثاره المحتملة على حقوق الإنسان للأفراد المعنيين أم لا.

ثالثا، تحقق جهات الإشراف الخارجي في الادعاءات بارتكاب مخالفات مرتبطة بالتعاون الدولي في مجال الاستخبارات. فعلى سبيل المثال، تقوم هذه الجهات بإجراء تحقيقات في الإجراءات التي اتخذتها أجهزة الاستخبارات في حالات معينة قد تعرض فيها أفراد لمعاملة سيئة.

## مربع ٧: المعايير الدولية المتعلقة بالاعتقال والاحتجاز

ينظم القانون الدولي عمليات القبض والاحتجاز من قبل جميع مؤسسات الدولة، بما في ذلك أجهزة الاستخبارات. وتحتوي معاهدات حقوق الإنسان الدولية، بما في ذلك العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR)، واتفاقية مناهضة التعذيب (CAT) عددا من الأحكام الرئيسية في هذا الصدد. كما أن مجموعة مبادئ الأمم المتحدة المتعلقة بحماية جميع الأشخاص الذين يتعرضون لأي شكل من أشكال الاحتجاز أو السجن (مبادئ الأمم المتحدة المعنية بمسألة الاحتجاز) تكمل القواعد الواردة في هذه المعاهدات<sup>١٠</sup>. وفي حين أن معظم الدول الديمقراطية لا تسمح لأجهزة استخباراتها باعتقال أو احتجاز أي شخص، وحتى إذا ما أُعطيت أجهزة الاستخبارات هذه الصلاحيات، فيتعين عليها الامتثال للمعايير الدولية التالية.

### الأساس القانوني للاعتقال والاحتجاز

- لكل فرد الحق في الحرية وفي الأمان على شخصه. ولا يجوز توقيف أحد أو اعتقاله تعسفاً. ولا يجوز حرمان أحد من حريته إلا لأسباب ينص عليها القانون وطبقاً للإجراء المقرر فيه. (العهد، المادة ٩-١)

### المعايير الإجرائية للاعتقال والاحتجاز

- لا يجوز إلقاء القبض أو الاحتجاز أو السجن إلا مع التقيد الصارم بأحكام القانون وعلى يد موظفين مختصين أو أشخاص مرخص لهم بذلك.. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٢).
- يتوجب إبلاغ أي شخص يتم توقيفه بأسباب هذا التوقيف لدى وقوعه كما يتوجب إبلاغه سريعا بأية تهمة توجه إليه. (الدولي الخاص بالحقوق المدنية والسياسية، المادة ٩-٢)
- تسجل حسب الأصول:
  - أ. أسباب القبض،
  - ب. وقت القبض ووقت اقتياد الشخص المقبوض عليه إلى مكان الحجز وكذلك وقت مثوله لأول مرة أمام سلطة قضائية أو سلطة أخرى،
  - ج. هوية موظفي إنفاذ القوانين المعنيين،
  - د. المعلومات الدقيقة المتعلقة بمكان الحجز.
- تبلغ هذه المعلومات إلى الشخص المحتجز أو محامية، إن وجد، بالشكل الذي يقرره القانون. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ١٢).
- تسجل وتعتمد بالطريقة التي يحددها القانون مدة أي استجواب لشخص محتجز أو مسجون والفترات الفاصلة بين الاستجوابات وكذلك هوية الموظفين الذين يجرون الاستجوابات وغيرهم من الحاضرين.. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٣٢-١).
- يحق للشخص المحتجز أن يحصل على مساعدة محام. وتقوم السلطة المختصة بإبلاغه بحقه هذا فور إلقاء القبض عليه وتوفر له التسهيلات المعقولة لممارسته. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٧١-١).
- يكون للشخص المحتجز أو المسجون، بعد إلقاء القبض عليه مباشرة وبعد كل مرة ينقل فيها من مكان احتجاز أو من سجن إلى آخر، الحق في أن يخطر، أو يطلب من السلطة المختصة أن تخطر أفرادا من أسرته أو أشخاصا مناسبين آخرين يختارهم، بالقبض عليه أو احتجازه أو سجنه أو بنقله وبالمكان الذي هو محتجز فيه.. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٦١-١).

### معايير لحماية الأشخاص المحتجزين

- يعامل جميع المحرومين من حريتهم معاملة إنسانية، تحترم الكرامة الأصلية في الشخص الإنساني. (العهد، المادة ١٠)
- لا يجوز إخضاع أي شخص يتعرض لأي شكل من أشكال الاحتجاز أو السجن للتعذيب أو غيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة. ولا يجوز الاحتجاج بأي ظرف كان كمبرر للتعذيب أو غيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٦، والمادة ٧ من العهد، والمادة ٢-٢-٣ من اتفاقية مناهضة التعذيب)
- يحظر استغلال حالة الشخص المحتجز أو المسجون استغلالاً غير لائق بغرض انتزاع اعتراف منه أو إرغامه على تجريم نفسه بأية طريقة أخرى أو الشهادة ضد أي شخص آخر. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ١٢-١)
- لا يعرض أي شخص أثناء استجوابه للعنف أو التهديد أو لأساليب استجواب تنال من قدرته على اتخاذ القرارات أو من حكمه على الأمور. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ١٢-٢)
- تبقى كل دولة قيد الاستعراض المنظم قواعد الاستجواب، وتعليماته وأساليبه وممارساته، وكذلك الترتيبات المتعلقة بحجز ومعاملة الأشخاص الذين يتعرضون لأي شكل من أشكال التوقيف أو الاعتقال أو السجن في أي إقليم يخضع لولايتها القضائية، وذلك بقصد منع حدوث أي حالات تعذيب. (اتفاقية مناهضة التعذيب، المادة ١١)

### الإشراف على الاحتجاز ومراجعته

- لا يتم أي شكل من أشكال الاحتجاز أو السجن ولا يتخذ أي تدبير يمس حقوق الإنسان التي يتمتع بها أي شخص يتعرض لأي شكل من أشكال الاحتجاز أو السجن إلا إذا كان ذلك بأمر من سلطة قضائية أو سلطة أخرى أو كان خاضعا لرقابتها الفعلية. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٤)
- لكل شخص حرم من حريته بالتوقيف أو الاعتقال حق الرجوع إلى محكمة لكي تفصل هذه المحكمة دون إبطاء في قانونية اعتقاله، وتأمراً بالإفراج عنه إذا كان الاعتقال غير قانوني. (العهد، المادة ٩-٤)
- لكل شخص كان ضحية توقيف أو اعتقال غير قانوني الحق في الحصول على تعويض. (العهد، المادة ٩-٥)
- تضمن كل دولة طرف لأي فرد يدعى بأنه قد تعرض للتعذيب [...] الحق في أن يرفع شكوى إلى سلطاتها المختصة وفي أن تنظر هذه السلطات في حالته على وجه السرعة وبنزاهة. (اتفاقية مناهضة التعذيب، المواد ٢١-٣١)
- لمراقبة مدى دقة التقيد بالقوانين والأنظمة ذات الصلة، يقوم بتفقد أماكن الاحتجاز بصفة منتظمة أشخاص مؤهلون ومتمرسون تعيينهم وتسلّمهم سلطة مختصة مستقلة تماما عن السلطة التي تتولى مباشرة إدارة مكان الاحتجاز أو السجن. (مبادئ الأمم المتحدة المعنية بالاحتجاز، المبدأ ٩٢-١)

### القوانين

المعتقل على محام وأن يكون قادرا على الاتصال بأسرته. أيضا، يجب أن تكفل أجهزة الاستخبارات للمعتقل ظروف المعيشة الكافية أثناء وجوده رهن الاعتقال والامتناع عن أي شكل من أشكال المعاملة السيئة للمحتجزين.

### الإشراف

لا شك أن الإشراف القضائي على عمليات الاحتجاز أمر ضروري للحيلولة دون اعتقال الأفراد تعسفاً. ويتطلب هذا الإشراف وجود محكمة للنظر في قانونية جميع الاعتقالات، وتكون هذه المحكمة، وليس ضابط الاستخبارات الذي اعتقل واحتجز الأفراد، هي من تحدد ما إذا كانت هناك أسباب مشروعة لاستمرار الاحتجاز أم لا. وإذا لم يتم اتهام

يحظر القانون على أجهزة الاستخبارات اعتقال واحتجاز المواطنين لمجرد جمع المعلومات. غير أن القانون قد يسمح، في ظروف خاصة، لأجهزة الاستخبارات باعتقال واحتجاز الأفراد الذين ارتكبوا جريمة ضد الأمن القومي أو يشكلون تهديداً حالياً أو وشيكاً على الأمن القومي.

### معاملة المحتجزين

يتعين على أجهزة الاستخبارات احترام حقوق الإنسان الواجبة للفرد المقبوض عليه أو المعتقل. وهناك إجراءات يجب أن تتخذ وأخرى يتعين الامتناع عنها. فعلى سبيل المثال، يجب على أجهزة الاستخبارات التأكد من حصول الشخص

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

جريمة جنائية خطيرة. بالإضافة إلى ذلك، قد يطلب ضباط الاستخبارات مصاحبة الشرطة لهم في المهام التي يمكن أن تهدد سلامتهم البدنية. على سبيل المثال، يجوز مرافقة ضابط شرطة لضابط الاستخبارات أثناء تنفيذ أمر قضائي لإزالة شيء ما أو تثبيت جهاز تنصت في منزل خاص.

تسمح بعض الدول الديمقراطية لأجهزة الاستخبارات استخدام صلاحيات الاعتقال والاحتجاز (انظر صفحة ٢٨). إذا واجه، أثناء تنفيذ عملية اعتقال، ضباط الاستخبارات تهديد وشيك على حياتهم أو حياة الآخرين، فيجوز لهم استخدام القوة المميتة. في مثل هذه الحالات، مع حتمية الامتثال لنفس القوانين والأنظمة التي تنطبق على استخدام القوة من جانب وكالات إنفاذ القانون (انظر مربع ٨). وهذا يعني أن أي استخدام للقوة يجب أن يكون لضرورة قصوى ومتناسبة مع الخطر. بالإضافة إلى ذلك، يجب على أجهزة الاستخبارات، مثلها مثل وكالات إنفاذ القانون، رفع تقارير عن كل حالة استخدام للقوة المميتة، على أن يخضع ذلك لتحقيق من جانب هيئة مستقلة.

## الرقابة والإشراف على أجهزة الاستخبارات

### لماذا تمارس المجتمعات الديمقراطية الرقابة على أجهزة الاستخبارات الخاصة بهم؟

هناك أربعة أسباب رئيسية تبرر مراقبة المجتمعات الديمقراطية لأجهزة الاستخبارات الخاصة بها، أولها أن المجتمعات الديمقراطية تضع القادة المنتخبين محل المساءلة عن عمل جميع الوكالات الحكومية والهيئات الممولة من المال العام. ولا تعتبر أجهزة الاستخبارات استثناء من هذه القاعدة. فيجب أن تراقب المجتمعات عمل أجهزة الاستخبارات للتأكد من مصداقية صرف الأموال العامة على تعيين الموظفين وتمويل الأنشطة فيها.

ثانياً، تتمتع أجهزة الاستخبارات بصلاحيات خاصة لجمع المعلومات التي لا تتوافر لغيرها من أعضاء المجتمع، وهي الصلاحيات التي تتيح إمكانية انتهاك حقوق الإنسان. ولذلك، فإن المجتمع الديمقراطي يراقب أجهزة الاستخبارات من أجل حماية حقوق الإنسان لجميع الأفراد الذين يتعاملون مع أجهزة الاستخبارات.

ثالثاً، أن دورها في جمع المعلومات يتيح لها إمكانية إعاقة الأحزاب السياسية ووسائل الإعلام وغيرها من

المحتجزين بارتكاب جريمة جنائية، يجب إطلاق سراحهم. إضافة إلى ما تقدم، تتفقد مؤسسات التحقيق في الشكاوى أو حقوق الإنسان مراكز الاحتجاز حيث يجوز لهذه المؤسسات في الكثير من الدول أن تجري زيارات غير معلنة لضمان معاملة المحتجزين معاملة لائقة.

## هل أجهزة الاستخبارات بحاجة إلى مراكز احتجاز خاصة بها؟

لا تسمح المجتمعات الديمقراطية لأجهزة الاستخبارات باستخدام مراكز احتجاز خاصة بها. ففي الدول التي تعطي صلاحيات الاعتقال والاحتجاز لأجهزة الاستخبارات، تستخدم هذه الأجهزة نفس مراكز الاحتجاز التي تستخدمها جهات تطبيق القانون. ومن بين فوائد استخدام هذه المراكز المشتركة مرافق الاحتجاز ضمان أن ضباط الاستخبارات لا يحتجزون الأفراد بشكل تعسفي وأنهم يعاملونهم وفقاً للقوانين الوطنية التي تعترف بالمعايير المقبولة دولياً بشأن معاملة الأشخاص رهن الاحتجاز.

## استخدام القوة المميتة من قبل أجهزة الاستخبارات

### هل يسمح لأجهزة الاستخبارات بالقتل؟

لا يسمح لأجهزة الاستخبارات بالقتل. إن القانون الدولي يحظر على الدول قتل أي شخص إلا في ثلاث حالات فقط وفي ظل ضوابط وقيود محددة: (١) في نزاع مسلح، يجوز لمحارب أن يقتل عدواً محارباً، ولكن ذلك يتوقف على الوفاء بمجموعة واضحة من الشروط. (٢) يجوز لسطات إنفاذ القانون استخدام القوة المميتة إذا كانت هناك ضرورة قصوى لمنع حدوث تهديد وشيك على الحياة، وليس هناك وسيلة أخرى لمواجهة هذا التهديد. (٣) في أعقاب العملية القضائية، يجوز للمحكمة أن تفرض عقوبة الإعدام بوصفها شكلاً من أشكال الإعدام في جرائم جنائية خطيرة محددة.

لا تسمح معظم الدول الديمقراطية لضباط الاستخبارات استخدام القوة من أي نوع. وفي الواقع، يخضع ضباط الاستخبارات لنفس القواعد الخاصة باستخدام القوة كأفراد من الجمهور. ويجب على أجهزة الاستخبارات طلب المساعدة من الشرطة في حالة الحاجة إلى استخدام القوة. جدير بالذكر أن أجهزة الاستخبارات قد تطلب من الشرطة القبض على شخص ارتكب أو على وشك ارتكاب

مربع ٨: المعايير الدولية بشأن استخدام القوة من جانب الموظفين الحكوميين

المقتطفات التالية من العهد ومدونة الأمم المتحدة لقواعد سلوك الموظفين المكلفين بإنفاذ القوانين ومبادئ الأمم المتحدة الأساسية بشأن استخدام القوة والأسلحة النارية من جانب الموظفين المكلفين بإنفاذ القوانين تنطبق على أجهزة الاستخبارات كلما تعين عليهم استخدام القوة ضد أي شخص<sup>١١</sup>. فإذا أعطت الدول أجهزة الاستخبارات صلاحيات الاعتقال والاحتجاز، فينبغي عليها التأكد من أنها مطابقة لهذه المعايير، فضلا عن سائر القوانين الوطنية والدولية المطبقة الأخرى.

- الحق في الحياة حق لازم لكل إنسان. وعلى القانون أن يحمي هذا الحق. ولا يجوز حرمان أحد من حياته تعسفا. (العهد، المادة ٦-١)
- لا يجوز للموظفين المكلفين بإنفاذ القوانين استعمال القوة إلا عند الضرورة القصوى وفي الحدود اللازمة لأداء واجبهم (مدونة قواعد سلوك المسؤولين عن إنفاذ القانون، المبدأ ٣).
- لا يجوز للموظفين المكلفين بإنفاذ القوانين استخدام الأسلحة النارية ضد الأشخاص إلا في حالة الدفاع عن النفس أو الدفاع عن الآخرين ضد تهديد وشيك بالموت أو الإصابة الخطيرة أو لمنع ارتكاب جريمة بالغة الخطورة تنطوي على تهديد خطير للحياة أو للقبض على شخص يشكل مثل هذا الخطر ويقاوم سلطتهم أو لمنع فراره ويكون ذلك فقط عندما تكون الوسائل الأقل شدة غير كافية لتحقيق هذه الأهداف. وعلى أية حال، لا يجوز استخدام الأسلحة النارية القاتلة عن قصد إلا عندما يتعذر تماما تجنبها من أجل حماية الأرواح. (مبادئ استخدام القوة والأسلحة النارية، المبدأ ٩)
- عندما يكون الاستخدام المشروع للقوة والأسلحة النارية أمر لا مفر منه، لا يجوز للموظفين المكلفين بإنفاذ القوانين:
  - أ- ضبط النفس في ممارسة مثل هذا الاستخدام والتصرف على نحو يتناسب مع خطورة الجرم والهدف المشروع؛
  - ب- تقليل الأضرار والإصابات واحترام وصون حياة الإنسان؛ (مبادئ استخدام القوة والأسلحة النارية، المبدأ ١١)
- تضمن الحكومات معاقبة مسؤولي إنفاذ القانون على الاستخدام المسيء أو التعسفي للقوة والأسلحة النارية بوصفه جريمة جنائية بموجب قوانينها. (مبادئ استخدام القوة والأسلحة النارية، المبدأ ٧)
- تضمن الحكومات وجهات إنفاذ القانون إجراء عملية مراجعة فعالة مع السماح للسلطات الإدارية أو سلطات الادعاء من ممارسة اختصاصها في ظروف مناسبة. (مبادئ استخدام القوة والأسلحة النارية، المبدأ ٢٢)
- يكون للأشخاص المتضررين من جراء استخدام القوة والأسلحة النارية أو ممثليهم القانونيين الحق في الوصول إلى عملية مستقلة، بما في ذلك العملية القضائية. (مبادئ استخدام القوة والأسلحة النارية، المبدأ ٣٢).

إمكانية وقوع الممارسات غير القانونية أو غير الفعالة تزيد نسبتها. وبالتالي، يتعين على الحكومات مراقبة العمليات السرية لضمان أن أجهزة الاستخبارات تؤدي عملها بفعالية ووفقا للقانون.

**ما هي المؤسسات التي تراقب و / أو تشرف على أجهزة الاستخبارات؟**

هناك خمسة أنواع رئيسية من المؤسسات تراقب و / أو تشرف على أجهزة الاستخبارات: الإدارة الداخلية لجهاز الاستخبارات (صفحة ٣٣)، والسلطة التنفيذية (صفحة ٣٤-٣٣)، والقضاء (صفحة ٣٤)، والبرلمان (صفحة ٣٤-٣٥) وهيئات الإشراف ذات الخبرة (صفحة ٣٥-٤٣).

المؤسسات والمهن الأخرى. وكذا تحتاج الدولة لمراقبة أجهزة الاستخبارات لحماية العناصر الحيوية في المجتمع الديمقراطي.

رابعاً، تحتاج المجتمعات الديمقراطية لمراقبة أجهزة الاستخبارات لأن القانون يسمح لهم بالعمل سرا. فعلى سبيل المثال، يمكنهم التنصت سرا على اتصالات الأفراد أو تصوير منازلهم مرئياً أو من خلال الصور الفوتوغرافية، في الوقت الذي قد لا دري فيه هذا الفرد بأن أجهزة الاستخبارات تتخذ تدابير ضده، ومن ثم لا يكون في موقف يسمح له باعتراض على هذه الإجراءات. وعلاوة على ذلك، فإنه من غير المرجح للأفراد والجمهور عموماً مراقبة أعمال أجهزة الاستخبارات التي تتم في الخفاء حتى عندما تتسم بالقانونية. وبالنظر إلى أن أجهزة الاستخبارات لا تخضع لنفس المستوى من التدقيق العام على عكس غيرها من الوكالات الحكومية، فإن

تقديم تقارير إلى البرلمان و / أو السلطة التنفيذية حول أنشطتها على أساس دوري ككل ستة أشهر مثلا. ويمكن للجهات الإشرافية البرلمانية أو ذات الخبرة طلب تقارير إضافية من أجهزة الاستخبارات أو من الوزير التنفيذي المسؤول عن أجهزة الاستخبارات حول قضايا معينة.

### من الذي يعين مديري الاستخبارات؟

توضح القوانين الوطنية الخطوط العريضة لإجراءات تعيين مديري الاستخبارات والمؤهلات المطلوبة في المديرين. وعادة ما يقوم رئيس الحكومة أو الوزير المسؤول عن أجهزة الاستخبارات، بتعيين مديري أجهزة الاستخبارات. وفي كثير من الدول، يتعين على السلطة التنفيذية التشاور مع زعماء أحزاب المعارضة قبل تعيين المديرين. وقد يحتاجون أيضا إلى التشاور مع البرلمان. يجوز للبرلمان طرح الأسئلة حول المرشح أو في بعض الحالات تنظيم جلسة معه أو معها. ولا شك أن إشراك أصحاب المصلحة الآخرين في تعيين المديرين يساعد على منع السلطة التنفيذية من تعيين الأشخاص الذين سوف يحمون أو يعززون مصالحهم السياسية الخاصة.

### لماذا يتم تعيين مديري الاستخبارات لمدة محددة؟

يشترط القانون تعيين مديري الاستخبارات لمدة محددة، ولا يمكن إقالته من منصبه إلا في حالة خرق قواعد محددة. وهذه الفترة المحددة تساعد على حماية مناصب المديرين من الضغوط السياسية أو التغييرات في الحكومة. فعلى سبيل المثال، تجعل هذه المدد المحددة من الصعب على أي من أعضاء السلطة التنفيذية فرض أجندته الخاصة على أجهزة الاستخبارات عن طريق التهديد بإقالة المدير من منصبه إذا لم ينتهج مسارا معينًا للعمل.

## السلطة التنفيذية

### ما هو دور السلطة التنفيذية في الرقابة على أجهزة الاستخبارات؟

في المجتمعات الديمقراطية، يكون للسلطة التنفيذية الرقابة الكاملة على أجهزة الاستخبارات. حيث يضع أعضاء السلطة التنفيذية سياسات وأولويات شاملة لأجهزة الاستخبارات. بالإضافة إلى ذلك، تكون السلطة التنفيذية هي المسؤولة سياسيا عن أجهزة الاستخبارات، بل هي المسؤولة أمام البرلمان والجمهور عن أنشطة الاستخبارات.

## الإدارة الداخلية

### ما هو الدور الذي تؤديه الإدارة الداخلية في الرقابة على أجهزة الاستخبارات؟

تراقب الإدارة الداخلية أنشطة الاستخبارات اليومية، وتتأكد من أن ضباط الاستخبارات يؤدون عملهم على نحو فعال مع تلبية للمتطلبات التنفيذية. كذلك تتولى الإدارة مسؤولية امتثال الاستخبارات بالقوانين الوطنية والدولية ذات الصلة.

تضع الإدارة الداخلية إجراءات لتحديد والإبلاغ عن وتقييم جميع أنشطة الاستخبارات، وبالإضافة إلى ذلك، تصدر قواعد السلوك وغيرها من الإرشادات لموظفي الاستخبارات. وتقوم الإدارة الداخلية أيضا بتنسيق عمليات تقييم أداء الموظفين.

### من ترفع أجهزة الاستخبارات تقاريرها؟

ترفع أجهزة الاستخبارات تقاريرها للسلطة التنفيذية والبرلمان والجمهور. حيث يرفعون تقاريرهم إلى السلطة التنفيذية حول أنشطتها المستقبلية الجارية والمنجزة. وبدورها تستخدم السلطة التنفيذية تقارير الاستخبارات لتقييم ما إذا كانت تقي باختصاصاتها وتلبية الأولويات الشاملة لأجهزة الاستخبارات أم لا.

كذلك ترفع أجهزة الاستخبارات تقاريرها إلى البرلمان إما مباشرة أو عن طريق الوزير المسؤول عن الاستخبارات. ويستخدم البرلمان تقارير أجهزة الاستخبارات لتدقيق أنشطتها وإبلاغ صناع القرار بشأن بمخصصات الميزانية المقبلة لأجهزة الاستخبارات. وأحيانا ترفع أجهزة الاستخبارات تقاريرها إلى الجلسة العامة للبرلمان التي عادة ما تكون جلسة عامة.

أيضا أجهزة الاستخبارات تقاريرها إلى هيئات إشرافية مستقلة بشأن الاستخبارات؛ وغالبا ما تحتوي هذه التقارير على معلومات سرية. وفي بعض الأنظمة، تقدم أجهزة الاستخبارات و / أو الوزير أو الوزراء المسؤولين تقاريرها إلى لجنة معينة في البرلمان أو لجنة إشراف ذات خبرة تعمل خارج البرلمان.

تقدم أجهزة الاستخبارات أيضا تقارير للجمهور. حيث تؤدي هذه التقارير العامة إلى رفع مستوى الوعي بعمل أجهزة الاستخبارات وتعزيز ثقة الجمهور. وعادة ما تنشر هذه التقارير على مواقع أجهزة الاستخبارات.

وعادة ما يطلب القانون الوطني من أجهزة الاستخبارات

مطالبة المحاكم بالفصل في القضايا المرفوعة ضد الأشخاص المتهمين بالكشف عن معلومات سرية بصورة غير مشروعة من تلك التي تحتفظ بها الاستخبارات.

وأخيراً، يجز للسلطة التنفيذية في الدول الديمقراطية مطالبة القضاة الحاليين أو السابقين بإجراء تحقيقات قضائية في أحداث أو أنشطة وقعت في الماضي ذات صلة بأجهزة الاستخبارات.

## البرلمان

**ما هو دور البرلمان في الرقابة على أجهزة الاستخبارات والإشراف عليها؟**

### ١. التشريع

تضع البرلمانات مسودات القوانين وتعتمد القوانين التي تنظم أجهزة الاستخبارات وتقوم بإنشاء مؤسسات للإشراف عليها. وحال قيامهم بصياغة التشريعات الخاصة بأجهزة الاستخبارات، يحاول أعضاء البرلمان إدراج أحكام شاملة بشأن الرقابة الخارجية والمساءلة واحترام سيادة القانون وحقوق الإنسان. وتعكف البرلمانات كذلك على تدقيق، وإذا لزم الأمر، تعديل التشريعات المقترحة. وأخيراً، تحدد البرلمانات وتعديل الثغرات الموجودة في التشريعات القائمة.

### ٢. الرقابة على التمويل

تراقب البرلمانات أيضاً استخدام أجهزة الاستخبارات «للمال العام»، حيث توافق على الميزانيات المقبلة ومراجعة المصروفات الماضية. جدير بالذكر أيضاً أن البرلمانات توافق على المصروفات المتوقعة كل عام. وخلال هذه العملية، تكون قادرة على الاستفسار من السلطة التنفيذية عن سياساتها وأولوياتها المتعلقة بأجهزة الاستخبارات. ويكون للبرلمان القدرة على رفض أو الحد من التمويل إذا رفضت السلطة التنفيذية و / أو أجهزة الاستخبارات معالجة نقاط القلق المثارة. وهكذا، يستخدم البرلمان دورهم الإشرافي على الميزانية للتأثير في السياسات والإجراءات التي تتخذها أجهزة الاستخبارات.

وبالإضافة إلى الموافقة على المصروفات المحتملة، تشارك البرلمانات في مراجعة المصروفات السابقة الخاصة بأجهزة الاستخبارات. ويكون للبرلمانات في بعض الدول

كما تضطلع السلطة التنفيذية بمسؤولية التصريح بنشاطات الاستخبارات التي تشكل خطراً كبيراً على سلامة الأفراد وعلاقات الدولة الخارجية و / أو سمعتها. وحال التصريح بهذه الأنشطة، تتحمل السلطة التنفيذية المسؤولية السياسية وتضع أيضاً ضوابط إضافية على أجهزة الاستخبارات.

تشرف السلطة التنفيذية على أجهزة الاستخبارات للتأكد من أنها تؤدي وظائفها على نحو فعال وفقاً للقانون. وإذا كانت هناك مزامم وقوع أخطاء من جانب أجهزة الاستخبارات، يجوز للسلطة التنفيذية بدء التحقيقات في أنشطة استخباراتية معينة.

وفي حين تستند أنشطة أجهزة الاستخبارات إلى أنظمة أساسية، إلا أن السلطة التنفيذية تصدر لوائح للمساعدة في توضيح وتنفيذ القوانين. على سبيل المثال، يمكن للسلطة التنفيذية إصدار مبادئ توجيهية بشأن المعايير الأخلاقية على أساس الأنظمة الأساسية المتعلقة بخدمات الاستخبارات.

## السلطة القضائية

**ما هو دور السلطة القضائية في الرقابة على أجهزة الاستخبارات والإشراف عليها؟**

تلعب الهيئات القضائية دوراً هاماً في الرقابة على أجهزة الاستخبارات والإشراف عليها. حيث تقوم في كثير من الدول بالسماح والرقابة على استخدام الصلاحيات الخاصة لأجهزة الاستخبارات (انظر صفحة ١٩-٢٠ ومربع ٣). كذلك تقوم المحاكم بتسوية الشكاوى المقدمة ضد أجهزة الاستخبارات، وإذا اقتضى الأمر، تضع المحاكم وسائل الانتصاف اللازمة جراء ارتكاب أي مخالفات. (انظر صفحة ٤٣-٤٥). من خلال أحكامها، ترسي المحاكم معايير لضبط السلوك المستقبلي لأجهزة الاستخبارات.

تفصل المحاكم أيضاً في المسائل المتعلقة بالحصول على أو الكشف عن معلومات تتعلق بأجهزة الاستخبارات. ففي العديد من الدول الديمقراطية، يحق للأفراد ومنظمات المجتمع المدني طلب معلومات عن أي وكالة حكومية حيث إن الوصول إلى هذه المعلومات يمكّن المجتمع من الإشراف على أنشطة الحكومة، بما في ذلك أجهزة استخباراتها. ويجوز مطالبة المحاكم بالفصل في مثل هذه الدعاوى المتعلقة بالمعلومات التي تحتفظ بها أجهزة الاستخبارات أو المعلومات ذات الصلة بها. يتم اتخاذ هذه القرارات على أساس قوانين الوصول إلى / حرية المعلومات. بالإضافة إلى ذلك، يمكن

٣٥ و جدول ٢).

وعادة ما يعين البرلمان جهات الرقابة وتقوم برفع تقاريرها للبرلمان و / أو السلطة التنفيذية.

وعلى عكس أعضاء اللجان البرلمانية للإشراف على أجهزة الاستخبارات، عادة ما تتكون جهات الإشراف ذات الخبرة من كبار الشخصيات العامة (ليس من بينهم أعضاء البرلمان)، بما في ذلك أعضاء بارزين في المجتمع المدني وأعضاء سابقين وحاليين في السلطة القضائية وسياسيين سابقين.

### دراسة متعمقة لجهات الإشراف البرلمانية وذات الخبرة على أجهزة الاستخبارات

يبحث هذا القسم في الدور الذي تلعبه اللجان البرلمانية و جهات الإشراف ذات الخبرة على أجهزة الاستخبارات، حيث يجب عن التساؤلات التي تتعلق بصلاحياتها وسلطاتها ومواردها وتعاملها مع المعلومات المصنفة وعلاقتها بأجهزة الاستخبارات واستقلالها ووظائف كتابة التقارير وإضافة إلى مزايا وعيوب كلا من اللجان البرلمانية و جهات الإشراف ذات الخبرة.

### ما هي جوانب العمل الاستخباراتي التي ينبغي الإشراف عليها بواسطة جهات الإشراف البرلمانية و / أو الجهات ذات الخبرة؟

تشرف جهات الإشراف البرلمانية و / أو الجهات ذات الخبرة على جميع جوانب أجهزة الاستخبارات (انظر جدول ٢ للوقوف على أمثلة لذلك). حيث تركز على أربعة مجالات، هي:

#### ١. الإشراف على قانونية العمليات والسياسات

يقوم المشرفون بتقييم ما إذا كانت السياسات القائمة وجميع جوانب العمليات الاستخباراتية الجارية متوافقة مع القوانين الوطنية والمعايير الدولية أم لا، فضلا عن تقييمهم لما إذا كانت العمليات والأنشطة الاستخباراتية المنجزة قد استوفت المتطلبات القانونية أم لا. وأخيرا، يراجع المشرفون على خطط الاستخبارات فيما يتعلق بالعمليات المستقبلية وتحديد ما إذا كانت هذه الأنشطة تمثل للقوانين والأنظمة والمعايير الدولية أم لا.

لجان حسابات تراجع جميع المصروفات الحكومية، بينما في دول أخرى تكن هناك مؤسسات وطنية لمراجعة الحسابات تؤدي هذه المهمة تحت إشراف البرلمان.

### ٣. الإشراف على السياسات والأنشطة

تشرف البرلمانات أيضا على إدارة وسياسات والأنشطة التنفيذية الخاصة بأجهزة الاستخبارات للمساعد في التأكد من الوفاء باختصاصاتها على نحو فعال وفقا للقانون. ويتم تنظيم الرقابة البرلمانية على أجهزة الاستخبارات من خلال عدة طرق. ففي بعض الدول، تكون اللجان البرلمانية للدفاع أو الداخلية مسؤولة عن الإشراف على الاستخبارات، بينما يقوم عدد أكبر من الدول بإنشاء لجان برلمانية خاصة للإشراف على أجهزة الاستخبارات. (انظر صفحة ٣٥-٤٣) وفي أماكن أخرى، تميل البرلمانات أكثر إلى الإشراف غير المباشر على أجهزة الاستخبارات، حيث تصرح لجهة خارجية أو ذات خبرة بتنفيذ أنشطة إشرافية يومية على هذه الأجهزة. كما يجوز للبرلمان المشاركة في تعيين أعضاء الجهات الإشرافية ذات الخبرة والتي تقوم في كثير من البلدان الديمقراطية برفع تقاريرها إلى البرلمان والذي يمكنه بدوره اتخاذ إجراءات للتأكد من أن استنتاجات هذه الجهات وتوصياتها قد تم التعامل معها.

وأخيرا، تشرف البرلمانات على أجهزة الاستخبارات من خلال إجراء تحقيقات في أحداث أو أنشطة معينة ذات صلة بأجهزة الاستخبارات.

### جهات الإشراف ذات الخبرة

#### ما هو دور جهات الإشراف ذات الخبرة على أجهزة الاستخبارات؟

هناك عدد متزايد من الدول التي أنشأت جهات إشراف ذات خبرة للإشراف على أجهزة الاستخبارات من خلال كونها تكمل أو تحل محل جهات الرقابة البرلمانية. وتكون هذه الجهات مستقلة عن أجهزة الاستخبارات والسلطة التنفيذية والبرلمان، إذ ينصب تركيزها حصريا على الإشراف على أنشطة استخباراتية معينة. وعادة ما تتمتع هذه الجهات بصلاحيات الإشراف على قانونية عمل أجهزة الاستخبارات، مع إمكانية مراقبتها لفاعلية العمليات والممارسات الإدارية والتمويلات الخاصة بأجهزة الاستخبارات (انظر صفحة

جدول ٢: مقارنة بين هيئات إشرافية استخباراتية مختارة في بلجيكا وكندا وجنوب أفريقيا والمملكة المتحدة<sup>١٢</sup>

المملكة المتحدة	جنوب إفريقيا	كندا	بلجيكا	
لجنة الاستخبارات والأمن	اللجنة الدائمة المشتركة لشئون الاستخبارات	لجنة مراجعة الاستخبارات الأمنية	اللجنة الدائمة للمراجعة على وكالات الاستخبارات	الاسم
هيئة إشرافية برلمانية	هيئة إشرافية برلمانية	هيئة إشرافية ذات خبرة	هيئة إشرافية ذات خبرة	النوع
مفوض أجهزة الاستخبارات مفوض اعتراض الاتصالات محكمة سلطات التحقيق	المفتش العام للاستخبارات (المفتش العام)	المفتش العام لدائرة الاستخبارات الأمنية الكندية (المفتش العام)	لجنة بمجلس الشيوخ مسؤولة عن مراقبة اللجنة الدائمة للمراجعة على وكالات الاستخبارات	هيئات إشرافية أخرى ذات صلة
٩ أعضاء في البرلمان ينتمون إلى المجلسين لا يمكن أن يكونوا وزراء (أي أعضاء من السلطة التنفيذية).	١٥ عضوا في البرلمان	٢-٤ أعضاء لا يمكن أن يكونوا أعضاء في البرلمان.	٣ أعضاء يجب أن يكون بها على الأقل عضو واحد من كل مجموعة لغوية؛ لا يمكن تقلد منصب انتخابي.	التكوين
من قبل رئيس الوزراء بالتشاور مع زعيم أكبر أحزاب المعارضة.	يعينهم البرلمان من خلال التمثيل النسبي، وعلى أساس الترشيحات التي يقدمها الأحزاب.	من قبل السلطة التنفيذية بعد التشاور مع زعماء أحزاب المعارضة.	من قبل مجلس الشيوخ (الغرفة العليا للبرلمان).	تعيين الأعضاء
مدة مجلس النواب.	مدة مجلس النواب.	٥ سنوات قابلة للتجديد.	٥ سنوات قابلة للتجديد مرتين.	مدة المنصب

الصلاحية	مراجعة أنشطة وأساليب أجهزة الاستخبارات وقواعدها الداخلية وتوجيهاتها ينبغي على اللجنة ضمان ما يلي: (١) حماية الحقوق الدستورية وغيرها بواسطة أجهزة الاستخبارات، (٢) تنسيق وفعالية أجهزة الاستخبارات التحقيق في الشكاوى؛ تقديم المشورة بشأن مشاريع القوانين والمراسيم والتوجيهات.	مراجعة أداء أجهزة الاستخبارات وواجباتها ووظائفها مراجعة التوجيهات الصادرة عن مدير جهاز الاستخبارات؛ ولوائح الأجهزة واتفاقاتها مع الكيانات المحلية والأجنبية وتقارير الأجهزة والمفتش العام ينبغي على اللجنة ضمان ما يلي: (١) توافق أنشطة الأجهزة مع القانون الواجب التطبيق، (٢) عدم ممارسة الأجهزة سلطاتها بطريقة غير معقولة أو لا ضرورة لها توجيه الأجهزة أو المفتش العام لإجراء مراجعة لأنشطة محددة، أو إذا رأت أن ذلك سيكون غير مناسب، إجراء مثل هذه المراجعة بنفسها؛ التحقيق في الشكاوى.	- مراجعة الشؤون المالية لأجهزة الاستخبارات، بما في ذلك تقارير مكتب مراجعة الحسابات تلقي الشكاوى وتوجيه المفتش العام أو أجهزة الاستخبارات للتحقيق فيها؛ - مراجعة تقارير المفتش العام، - تقديم توصيات بشأن التشريعات ذات الصلة بالاستخبارات وأي مسألة أخرى تتعلق بالأمن القومي والاستخبارات.	- فحص نفقات وإدارة وسياسة أجهزة الاستخبارات.
سلطات التحقيق	يمكنها استدعاء أي شخص للإدلاء بشهادته تحت القسم أمام اللجنة؛ يمكن طلب المساعدة من سلطات إنفاذ القانون لإجبار الأشخاص على الامتثال.	عند التحقيق في الشكاوى، تتمتع هذه اللجنة بصلاحيات محكمة: يجوز لها استدعاء وإنفاذ مثول الأشخاص أمام اللجنة وإجبارهم على الإدلاء بشهادة شفوية أو مكتوبة تحت القسم.	يمكنها مطالبة أي وزير أو رئيس جهاز مخابرات أو مفتش عام للمثول أمامها؛ الحق في عقد جلسات استماع واستدعاء الشهود.	يمكنها استدعاء وزراء وغيرهم من الموظفين المختصين للإدلاء بشهاداتهم.

<p>يمكن للوزير المسؤول أن يحدد من وصول اللجنة إلى المعلومات الحساسة التي يمكن أن تكشف تفاصيل العمليات أو مصادر وأساليب أجهزة الاستخبارات.</p>	<p>فرض بعض القيود المفروضة على الوصول إلى المعلومات التي تحتفظ بها أجهزة الاستخبارات، وأسماء العملاء و / أو يمكن حجب مصادر عن اللجنة.</p>	<p>الوصول غير المحدود إلى جميع المعلومات اللازمة لأداء واجباتها ووظائفها.</p>	<p>الحصول على جميع المعلومات التي تراها ضرورية؛ يجب على أجهزة الاستخبارات، بمبادرة منها، تزويد اللجنة بجميع القواعد الداخلية والتوجيهات.</p>	<p><b>الحصول على معلومات سرية</b></p>
<p>مبادرة ذاتية؛ بناء على طلب من الوزير المسؤول.</p>	<p>يمكنها صياغة مسودة تقرير خاص بناء على طلب من البرلمان، أو الوزير المسؤول (الوزراء).</p>	<p>مبادرة ذاتية؛ شكوى.</p>	<p>مبادرة ذاتية؛ شكوى؛ بناء على طلب من البرلمان؛ بناء على طلب من الوزير المسؤول.</p>	<p><b>بواعث التحقيقات</b></p>
<p>تقرير سنوي إجباري؛ فضلا عن إمكانية إصدار تقارير بشأن أي مسألة ذات صلة؛ يتم إرسال جميع التقارير أولا لرئيس الوزراء الذي يقدمها بعد ذلك إلى البرلمان يقرر رئيس الوزراء ما هي المعلومات التي يجب حذفها من النسخة المعلنة من التقرير.</p>	<p>تقرير سنوي إجباري للبرلمان والرئيس والوزير المسؤول (الوزراء) لا يمكن أن تحتوي التقارير على معلومات قد تكون ضارة بالأمن القومي</p>	<p>- تقرير سنوي إجباري - تقارير تقدم أولا للسلطة التنفيذية التي يجب أن تضع التقرير أمام البرلمان في غضون ١٥ يوما إصدار تقارير خاصة عند طلب وزير أو من تلقاء نفسه وجوب التشاور مع مدير جهاز الاستخبارات العامة قبل الإعلان عن التقرير.</p>	<p>تقرير سنوي إجباري لرئيس مجلسي البرلمان والوزير المسؤول؛ تقارير خاصة تقدم أولا إلى الوزير المسؤول، ثم إلى مجلس الشيوخ تقارير مقدمة إلى البرلمان لا تحتوي على أي معلومات سرية.</p>	<p><b>تقديم التقارير</b></p>

## ٢. الإشراف على فعالية العمليات

يقوم المشرفون برصد فعالية العمليات الاستخباراتية مع تحديد ما إذا كانت أجهزة الاستخبارات تؤدي وظائفها وأنشطتها مهامها بشكل فعال وفقا للقانون والسياسات والأولويات التنفيذية أم لا.

## ٣. الإشراف على الممارسات الإدارية

يراقب المشرفون الممارسات الإدارية لأجهزة الاستخبارات، حيث يراجعون سياسات الموارد البشرية والممارسات الإدارية من بين أمور أخرى.

## ٤. الإشراف على الإدارة المالية

يراقب المشرفون الأنشطة المالية الداخلية لأجهزة الاستخبارات بما في ذلك ميزانياتها ومصروفاتها.

وفي بعض الأنظمة، تنشئ الدول جهة رقابة إما برلمانية أو ذات خبرة فقط لرصد وتقييم أنشطة أجهزة الاستخبارات. ومع ذلك، فإن الأكثر شيوعا أن تقوم الدول بإشراك أكثر من جهة إشراف لرصد جميع جوانب العمل الاستخباراتي. فعلى سبيل المثال، يمكن للدولة أن توكل للجنة الإشراف البرلماني مسؤولية رصد فعالية أنشطة الاستخبارات وإعطاء جهة

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

إلى الموارد البشرية والمالية للاضطلاع بدورها بفعالية. فهي تحتاج إلى تمويل كاف لتوظيف الموظفين الدائمين والاستعانة بخدمات خبراء معينين عند الحاجة. كما أنها بحاجة إلى تمويل لشراء المعدات كأجهزة الكمبيوتر. ونظرا لتعاملها مع معلومات حساسة للغاية، فهي بحاجة إلى معدات حاسوبية متطورة جدا وخبراء فنيين لإعداد أنظمة الأمن.

توظف هيئات الإشراف عاملين دائمين يؤدون الأدوار التي تعتبر أساسية لمنظمتهم. حيث يقوم العاملون بكثير من العمل اليومي لهيئات الإشراف، وتشمل مهامهم التحضير لعمليات التفتيش وإجراء تحليلات للأنشطة الاستخباراتية وتقديم تقارير عن تحقيقات هيئة الإشراف. وفي حين أن كلا من أعضاء الهيئات الإشرافية البرلمانية وذات الخبرة خبراء قد يتغيرون، إلا أن العاملين يظلون في كثير من الأحيان مع المنظمة لفترات أطول من الأعضاء، وبالتالي، فهم قادرين على ضمان استمرارية الأنشطة فضلا عن تزويد المنظمة بـ «الذاكرة المؤسسية». كما أن خدمتهم الطويلة أيضا تكفل لهم معرفة وخبرة متنامية بالعديد من جوانب العمل الاستخباراتي.

وعادة ما تختار هيئات الإشراف البرلمانية عامليها ممن يعملون بالفعل في البرلمان. بينما تعين هيئات الإشراف ذات الخبرة موظفيها من خارج الحكومة. ويجب في كلا الحالتين حصول العاملين على موافقات أمنية لضمان أنهم موثوق بهم للتعامل مع المعلومات الحساسة المتعلقة بأجهزة الاستخبارات.

ويتطلب الإشراف على أجهزة الاستخبارات خبرة ومعرفة بالممارسات المعقدة التي لا يجيدها سوى قلة قليلة ممن يعملون خارج دوائر الاستخبارات. لذلك، ففي بعض الحالات تحتاج هذه الجهات لتوظيف خبراء استخبارات لمساعدتها على القيام بالتحقيقات والتعامل بفعالية مع القضايا المعقدة المتصلة بالعمل الاستخباراتي. وبالمثل، فإنها تحتاج في كثير من الأحيان خبراء في تكنولوجيا المعلومات والاتصالات السلكية واللاسلكية مع خلفية استخباراتية لمساعدتهم على فهم أفضل للتقنيات الالكترونية المعقدة المستخدمة من قبل أجهزة الاستخبارات.

### كيف يراقب المشرفون أجهزة الاستخبارات؟

تستخدم جهات الإشراف البرلمانية وذات الخبرة أساليب مختلفة لرصد أنشطة أجهزة الاستخبارات، حيث تعتمد الأساليب المستخدمة على صلاحية جهة الرقابة وسلطاتها القانونية.

الإشراف ذات الخبرة مسؤولية مراقبة قانونية أنشطتها. وبغض النظر عن التكوين الدقيق لنظام الرقابة، تضمن الدول الديمقراطية وجود رقابة على جميع جوانب أنشطة أجهزة الاستخبارات من خلال واحدة أو أكثر من الجهات الخارجية.

### ما هي السلطات القانونية المكفولة للهيئات الإشرافية؟

تضمن المجتمعات الديمقراطية أن هيئات الإشراف البرلمانية وذات الخبرة تمارس أدوارها وصلاحياتها وسلطاتها استنادا إلى التشريعات (انظر جدول ٢ للأمتثلة). يشترط القانون على السلطة التنفيذية وأجهزة الاستخبارات على التعاون مع الهيئات الإشرافية، حيث إن هذا أمر ضروري في أداء دورها.

يمنح القانون هيئات الإشراف الصلاحيات اللازمة لمراقبة عمل أجهزة الاستخبارات، وهو أمر ضروري لمحاسبتهم على أعمالهم. فأولا، يعطي القانون الهيئات الإشرافية القدرة على العمل بشكل مستقل والشروع في تحقيقات ذاتية دون الحاجة إلى الحصول على إذن مسبق من السلطة التنفيذية أو أجهزة الاستخبارات.

ثانيا، يعطي القانون هيئات الإشراف حق الوصول الكامل إلى جميع المعلومات ذات الصلة بعملها، بما في ذلك الملفات السرية التي تحتفظ بها أجهزة الاستخبارات. ولا شك أن الوصول إلى هذه المعلومات ضروري لتحديد ما إذا كانت، من بين أمور أخرى، أجهزة الاستخبارات تعمل بفاعلية وفقا للقانون أم لا. وقد يعتبر عدم الامتثال لطلب هيئة الإشراف للمعلومات من جانب ضابط الاستخبارات جريمة جنائية بموجب القانون. وفي كثير من الدول، يجوز لهيئة الإشراف مطالبة سلطات إنفاذ القانون بإجبار الأفراد على الامتثال لطلباتها للحصول على المعلومات.

ثالثا، تتمتع هيئات الإشراف بسلطة استدعاء وزراء ومسؤولين عن أجهزة الاستخبارات لإعطاء أجوبة على أسئلتهم المتعلقة بعمل الاستخبارات. في دول كثيرة، يجب على هؤلاء الأفراد الإدلاء بشهاداتهم لهيئة الإشراف تحت القسم.

وأخيرا، تتمتع هيئات الإشراف بحرية زيارة مقر أجهزة الاستخبارات. ويمكن ترتيب هذه الزيارات مسبقا مع أجهزة الاستخبارات، أو بشكل غير معلن.

### لماذا تحتاج هيئات الإشراف إلى موارد مالية وبشرية؟

بالإضافة إلى الصلاحيات القانونية، تحتاج هيئات الإشراف

التنفيذية بشأن كيفية تحسين المساءلة والشفافية والشرعية والفعالية.

يجوز لجهات الرقابة تقديم تقارير إضافية في سنة معينة. وهي كذلك تعد تقارير خاصة تصف التحقيقات الخاصة بأحداث معينة أو مواضيع عامة. وعادة ما تقدم جهات الرقابة نسختين من تقاريرها: واحدة للسلطة التنفيذية وأجهزة الاستخبارات والتي قد تحتوي على معلومات سرية، ونسخة أخرى للجمهور عموماً لا تحتوي على معلومات سرية. وفي هذا الصدد، تتشاور جهات الرقابة مع السلطة التنفيذية وأجهزة الاستخبارات قبل طرح التقارير العامة حتى تتيح للسلطة التنفيذية وأجهزة الاستخبارات فرصة التعبير عن أي مخاوف لديها إذا كان التقرير يحتوي على معلومات حساسة.

### لماذا تعتبر التقارير العامة أمراً هاماً؟

أولاً، أن التقارير العامة من شأنها إعلام المجتمع بأنشطة أجهزة الاستخبارات، وفي الوقت نفسه تعزز فهم الجمهور وثقته في جهة الرقابة على الاستخبارات.

ثانياً، يستخدم المشرفون تقاريرهم في محاولة لإحداث تغيير داخل أجهزة الاستخبارات، بشأن السياسات التنفيذية الإستراتيجية أو التشريعات التي تنظم أنشطة الاستخبارات. وغالباً ما تحتوي تقارير جهات الرقابة على توصيات بشأن كيفية تحسين سياسات وممارسات معينة. ويمكن للمشرفين متابعة هذه التوصيات في السنوات اللاحقة لمحااسبة أجهزة الاستخبارات والسلطة التنفيذية حيال تعاملهم مع المشاكل التي تم تحديدها سابقاً في منظماتهم.

### هل هناك تضارب بين الحق في المعرفة والحاجة للحفاظ

#### على سرية المعلومات؟

تحتاج جهات الإشراف البرلمانية وذات الخبرة إلى معلومات مفصلة عن أنشطة أجهزة الاستخبارات من أجل الإشراف عليها. ففي معظم البلدان الديمقراطية، تتمتع الجهات الإشرافية بحق قانوني في الوصول إلى كل المعلومات ذات الصلة بعملهم في الوقت الذي تحتاج فيه أجهزة الاستخبارات إلى حماية المعلومات التي إن تم الكشف عنها قد تضرر بالتحقيقات الجارية أو تكشف الأساليب والمصادر المستخدمة لجمع المعلومات. كذلك فإن الكشف عن هذه المعلومات قد يضر أيضاً بالأمن القومي. ومن ثم تشعر أجهزة الاستخبارات في كثير من الأحيان بعدم الارتياح إزاء

فأولاً، تطلع هذه الجهات على تقارير سرية وغير سرية تقدمها أجهزة الاستخبارات، ومن ثم يحصلون على معلومات مفيدة تتعلق بجميع جوانب عمل الاستخبارات، وهو ما يحفز على المزيد من الأسئلة التي قد تؤدي إلى فهم أفضل للعمليات الداخلية.

ثانياً، تقوم هذه الجهات بأخذ عينات عشوائية من المعلومات التي عالجتها أو خزنتها أجهزة الاستخبارات. ويمكن أن يتم أخذ عينات عشوائية خلال عمليات تفتيش منتظمة أو من خلال زيارات مفاجئة. فعلى سبيل المثال، إذا رغبت هذه الجهات في تقييم ما إذا كانت أجهزة الاستخبارات تستخدم البيانات الشخصية وفقاً للقانون أم لا، فستقوم باختيار عشوائي لعدد من الملفات الفردية وفحصها لمعرفة ما إذا كانت هذه العينات تفي بالمطلبات أم لا.

ثالثاً، تجري هذه الجهات تحقيقات موضوعية لفحص مجال معين من عمل الاستخبارات بعناية. وتركز هذه التحقيقات عادة على مجالات واسعة بدلاً من أحداث أو أنشطة محددة. وفي كثير من الأحيان تقوم جهات الرقابة باختيار المواضيع بناء على دواعي قلق معينة نمت إلى علمها من قبل الجمهور أو كيانات حكومية وغير حكومية، وغالباً ما يكون ذلك لمتابعة التحقيقات أو عمليات التفتيش السابقة.

رابعاً، تقوم هذه الجهات بإجراء تحقيقات في وقائع أو ادعاءات محددة تتعلق بأجهزة الاستخبارات. وتبدأ التحقيقات في حوادث محددة من تلقاء نفسها أو حال وجود استفسارات ذات صلة من السلطة التنفيذية و / أو البرلمان. ويتم من خلال هذه التحقيقات مراجعة جميع المعلومات ذات الصلة التي تحتفظ بها أجهزة الاستخبارات فيما يتعلق بأحداث وادعاءات محددة.

وأخيراً، تقوم بعض جهات الإشراف البرلماني وذات الخبرة بالتحقيق في شكاوى محددة يتقدم بها الأفراد (انظر صفحة ٤٣-٤٥). ومن خلال التحقيق في شكاوى معينة، يتكون لدى المشرفين فهم لمشكلات أكبر في عمل أجهزة الاستخبارات حيث تتبّع الجهات الإشرافية الجوانب النمطية في الشكاوى التي تلقاها لتستخدمه كأساس لمزيد من التحقيقات.

### كيف تقدم جهات الإشراف تقارير عن أنشطتها؟

بشكل عام يشترط القانون على جهات الرقابة تقديم تقارير عامة سنوية عن أنشطتها. وتتضمن هذه التقارير عادة معلومات حول عضويتها الحالية والتحقيقات ونتائج التحقيقات بالإضافة إلى التقارير المالية والتوصيات. حيث ترشد هذه التوصيات أجهزة الاستخبارات والسلطة

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

البيانات الشخصية. ولا يجوز لهيئات الإشراف الكشف عنها إلا بموافقة الشخص المعني، وفقا للمعايير المحددة الأخرى المنصوص عليها في القانون.

### ما هي أهمية العلاقة بين أجهزة الاستخبارات وهيئات الإشراف؟

تسعى هيئات الإشراف بصفة عامة لإقامة علاقة بناءة مع أجهزة الاستخبارات التي يراقبونها. ويرجع ذلك للصعوبة البالغة التي يواجهها المشرفون في مراقبة أجهزة الاستخبارات كما ينبغي دون تعاونهم. يعتمد المشرفون على أجهزة الاستخبارات لتسهيل حصولهم على المعلومات اللازمة. ويمكن لهيئات الإشراف كسب ثقة أجهزة الاستخبارات من خلال معاملة المعلومات السرية برعاية وإبقائهم على علم بأنشطة الإشراف.

تستفيد أجهزة الاستخبارات أيضا من وجود علاقة عمل بناءة مع هيئات الإشراف. ويمكن لتقارير هيئات الإشراف أن تعزز شرعيتها وكسب ثقة الجمهور في عملهم. وفي بعض الحالات، يمكن أيضا أن تساعد تقارير هيئات الإشراف أجهزة الاستخبارات تبرير الحصول على موارد مالية أو بشرية إضافية. بالإضافة إلى ذلك، ففي حالة وجود ادعاءات حول أجهزة الاستخبارات، يمكن لتحقيق هيئات الإشراف أن يساعد في بعض الأحيان على إعادة بناء الثقة العامة فيها. ويمكن لهيئات الإشراف أيضا أن تلعب دورا في حماية أجهزة الاستخبارات ضد احتمالات إساءة استخدام السلطة من قبل المسؤولين التنفيذيين. ويمكن لمسؤولي الاستخبارات الإبلاغ عن الأمور غير ملائمة أو غير قانونية التي تتلقاها من هيئة الإشراف. وبالنظر إلى هذه الفوائد، نجد أن من مصلحة أجهزة الاستخبارات عموما التعاون مع هيئات الإشراف.

وفي حين أن علاقة العمل يجب أن تكون بناءة، إلا أنه ينبغي تجنب القرب الشديد في هذه العلاقات حيث إن الجمهور سيرى هيئات الإشراف مستقلة وفعالة إذا ما حافظت على مسافة معينة بينها وبين أجهزة الاستخبارات.

### كيف تضمن المجتمعات الديمقراطية استقلالية هيئات الإشراف على الاستخبارات؟

تعتبر هيئات الإشراف البرلمانية وذات الخبرة منظمات مستقلة ولا يمكن أن يكونوا جزءا من السلطة التنفيذية أو أجهزة الاستخبارات، لأنها يجب عليها الإشراف على من يقوم بجمع واستخدام المعلومات الاستخباراتية.

منح المشرفين حق الوصول الكامل إلى المعلومات الخاصة بهم لأنهم يخشون إمكانية تسرب معلومات سرية.

إلى جانب ذلك، ينتاب العديد من أجهزة الاستخبارات القلق من أن المشرفين قد يقوضون التزامات السرية بشأن البيانات الشخصية. ويشترط القانون على أجهزة الاستخبارات وموظفيها التعامل مع البيانات الشخصية بسرية كما يقيد تبادل مثل هذه المعلومات.

ونظرا لتضارب هذه المطالب بشأن المعلومات التي تحتفظ بها أجهزة الاستخبارات، تظهر احتمالية نشوب صراع بين أجهزة الاستخبارات والمشرفين فيما يتعلق بالحصول على المعلومات. ومع ذلك، يمكن اتخاذ عدة تدابير لمنع مثل هذه الصراعات (انظر صفحة ٤١).

### كيف يمكن التوفيق بين احتياجات جهات الإشراف والاستخبارات؟

توجد تدابير خاصة لضمان تعامل جهات الإشراف مع المعلومات السرية بشكل مناسب. وهذه التدابير تساعد على طمأنة أجهزة الاستخبارات حيال عدم تسريب المشرفين للمعلومات السرية.

أولا، تعقد هيئات الإشراف البرلمانية وذات الخبرة اجتماعاتها سرا مع عدم الإفصاح عن محتوى هذه الاجتماعات.

ثانيا، جرت العادة في الدول الديمقراطية أن تجرم القوانين الكشف عن المعلومات السرية بوصفها جريمة جنائية. وفي العديد من الدول يتعين على أعضاء وموظفي هيئات الإشراف وموظفيها الحصول على تصاريح أمنية، وهو ما يعني أنه يتم التحري عنهم لضمان مدى إمكانية الوثوق بهم عند الوصول إلى المعلومات السرية. بالإضافة إلى ذلك، يجوز مطالبة المشرفين بالتوقيع على اتفاقات تنص على عدم كشفهم للمعلومات السرية.

ثالثا، تحتاج جهات الإشراف إلى اتخاذ تدابير لمنع موظفيها من الكشف عن المعلومات السرية، وغالبا ما تطبق سياسات تحظر على الأعضاء والموظفين نقل معلومات سرية إلى خارج المقر. أيضا، هناك تدابير أمنية خاصة يمكن اتخاذها لحماية الوثائق الورقية والالكترونية التي تحتوي على معلومات حساسة.

وأخيرا، تنطبق قوانين حماية البيانات الشخصية على هيئات الإشراف، كما هو الحال في أي مؤسسة عامة أخرى. يشترط القانون على هيئات الإشراف الحفاظ على سرية

وعادة ما ينظم القانون عملية اختيار وتعيين أعضاء هيئات الإشراف. في كثير من الدول، يعين البرلمان أعضاء هيئات الإشراف. وهذا يعني أن يتم اختيار المشرفين من قبل مؤسسة مستقلة عن تلك الخاضعة للإشراف. ويعد هذا الأمر ضروريا لضمان استقلال الأشخاص الذين يعملون في هيئات الإشراف. وفي عدد قليل من الدول، تتولى السلطة التنفيذية مسؤولية تعيين أعضاء هيئات الإشراف ولكن خياراته تحتاج إلى موافقة البرلمان، وفي بعض الحالات القضاء.

كذلك فإن تعيين أعضاء هيئات الإشراف لمدة محددة يعطيهم استقلالية إضافية ويحميهم من الضغوط الخارجية. ولما كانت هذه المدد محددة بموجب القانون، فلا يمكن للسياسيين فصل الموظفين تعسفا، إذ لا يجوز الفصل إلا إذا كان الشخص المعني قد ارتكب جريمة خطيرة أو فشل في أداء واجباته. وفي بعض البلدان، لا يسمح القانون لأعضاء هيئات الإشراف بالعمل لمدة ثانية. ويسعى المشرعون من وراء تحديد مدد المناصب إلى منع أعضاء هيئات الإشراف من إساءة استخدام مناصبهم وذلك بهدف التأثير على قرارات إعادة تعيينهم.

وكتدبير إضافي لضمان الاستقلالية، قد يحظر القانون تولي أعضاء هيئات الإشراف مناصب أخرى. ولأسباب واضحة، لا يمكن تعيين أعضاء هيئات الإشراف في أجهزة الاستخبارات. وقد يحظر القانون أيضا على المشرفين العضوية في حزب سياسي أو المشاركة في الأنشطة التجارية، مما يساعد على منع حدوث تضارب محتمل في المصالح.

### ما هي مزايا هيئات الإشراف البرلمانية؟

تتمتع هيئات الإشراف البرلمانية بأثنتين من المزايا الرئيسية مقارنة بالهيئات ذات الخبرة. أولها وأهمها أنها تتمتع «بشرعية ديمقراطية» أكثر لأنها منفذة من قبل أفراد منتخبين، ممن يشرفون على أجهزة الاستخبارات ولديهم علاقة مباشرة مع الجمهور. وعلى النقيض من ذلك، يتمتع أعضاء هيئات الإشراف ذات الخبرة بشرعية غير مباشرة فقط، لأنه عادة ما يتم اختيارها إما عن طريق البرلمان أو السلطة التنفيذية.

ثانيا، تتقلد هيئات الإشراف البرلمانية وضعا أفضل للتأثير بشكل مباشر على سياسات وأنشطة السلطة التنفيذية وأجهزة الاستخبارات. وللبرلمان أداتين رئيسيتين تحت تصرفه في هذا الصدد: قدرته على تمرير أو تعديل تشريع

تعتمد الدول الديمقراطية قوانين تكفل لهيئات الإشراف على أجهزة الاستخبارات هوية قانونية مستقلة حيث تهدف هذه القوانين إلى حماية استقلالها التنظيمي والتشغيلي. كما أن هذه القوانين تسمح لهيئات الإشراف أداء أنشطتها دون تدخل من السلطة التنفيذية أو أجهزة الاستخبارات. على سبيل المثال، يمكنها تحديد الحالات أو المواضيع التي سيتم التحقيق فيها وتحديد الكيفية التي سيتم بها إجراء التحقيقات. وتعني الهوية القانونية المستقلة لهيئات الإشراف أنها لا تتلقى أي تعليمات من السلطة التنفيذية أو أجهزة الاستخبارات.

يمكن لهيئات الإشراف أن تقرر أيضا بشكل مستقل المعلومات التي تحتاج إلى الوصول إليها من أجهزة الاستخبارات. وتكفل هذه الضمانة القانونية في الحصول على المعلومات عدم تحكم أجهزة الاستخبارات ولا السلطة التنفيذية في عمل هيئات الإشراف من خلال تقييد وصولهم إلى المعلومات. وفي بعض الحالات، قد تعتمد هيئات الإشراف على المحاكم في مطالبة أجهزة الاستخبارات بمنحها فرص الحصول على المعلومات ذات الصلة.

ويمكن أيضا لهيئات الإشراف اتخاذ قرارات مستقلة تتعلق بتقديم التقارير. وعمليا، يتشاور المشرفون مع أجهزة الاستخبارات والسلطة التنفيذية قبل نشر التقارير. ومع ذلك، فإن السلطة التنفيذية وأجهزة الاستخبارات ليس لها اللجوء إلى القضاء لوقف هيئات الإشراف من نشر النتائج المستقلة التي توصلوا إليها والتوصيات الواردة في التقارير.

في العديد من الدول الديمقراطية، تتمتع هيئات الإشراف على الاستخبارات أيضا بميزانية مستقلة، وهذا يعني أنها يمكنها طلب تمويلها من البرلمان وإدارة ميزانياتها الخاصة. ونظرا لاستقلالها ماليا، لا يمكن لغيرها من المنظمات (مثل السلطة التنفيذية وأجهزة الاستخبارات) التأثير على قراراتها من خلال تهديدهم بتخفيض التمويل.

### كيف يمكن ضمان استقلال أعضاء هيئات الإشراف؟

لا يمكن استقلال هيئة الإشراف إلا بالحفاظ على استقلال أعضائها وموظفيها. وهذا يعني أنهم لا سيجئون استخدام مناصبهم لتحقيق مكاسب شخصية أو لتعزيز مصالح الآخرين. وهكذا، تعتمد المجتمعات الديمقراطية قوانين لضمان الحفاظ على استقلالية الأفراد المعينين في هيئات الإشراف.

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

مناصبهم بشكل أكبر وبالتالي لا يتكون لديهم نفس القدر من المعرفة والخبرة.

وأخيرا، لما كان أعضاء هيئات الإشراف ذات الخبرة بشكل عام أقل عرضة للتأثير السياسي، فهم أيضا أقل عرضة لتسريب المعلومات الحساسة لأغراض سياسية. كذلك فإن عدد البرلمانين العاملين في اللجان المكفول لها إمكانية الحصول على معلومات سرية أكثر كثيرا مقارنة بأعضاء هيئات الإشراف ذات الخبرة. وهكذا، تكون اللجان البرلمانية أكثر عرضة لإساءة استخدام المعلومات الحساسة لأسباب سياسية مثل تسريب معلومات لتشويه سمعة معارضين سياسيين. ومن هنا تضع أجهزة الاستخبارات قيودا أكبر على أمن المعلومات الخاصة بهم. وفي كثير من الدول، عادة ما تنعدم ثقة أجهزة الاستخبارات في البرلمان وربما يخشون من إمكانية تسريب أعضاء لجان الإشراف البرلمانية لمعلومات سرية.

### الشكاوى ضد أجهزة الاستخبارات

#### كيف يمكن للجمهور التقدم بشكاوى ضد أجهزة الاستخبارات؟

في المجتمعات الديمقراطية، يحق للأفراد تقديم شكاوى حول أي إجراء يتخذ ضدهم من قبل مؤسسة عامة، بما في ذلك أجهزة الاستخبارات. ويمكن لأي شخص الطعن في أي إجراء تتخذه الاستخبارات ضدهم، بما في ذلك الاعتقال والاحتجاز وتفتيش منازلهم أو اعتراض الاتصالات الخاصة بهم.

يمكن للأشخاص الذين يعتقدون أنهم تعرضوا لظلم أو معاملة غير قانونية من قبل أجهزة الاستخبارات تقديم شكاواهم لدى هيئة مستقلة. (انظر مربع ٩ للحصول على مثال لكيفية التعامل مع الشكاوى ضد أجهزة الاستخبارات). وعادة ما يتم التعامل مع هذه الشكاوى بواسطة محكمة أو هيئة غير قضائية، مثل محقق الشكاوى أو هيئة إشراف ذات خبرة على الاستخبارات. ويتعين على هذه الهيئة تقييم ما إذا كان جهاز الاستخبارات اتخذ إجراءات ضد الشخص المعني أم، وإذا كان الأمر كذلك، هل استخدم الجهاز سلطاته وفقا للقانون أم لا.

وإذا وجدت الهيئة النازرة في الشكاوى أن الشكاوى صحيحة، فيمكنها مطالبة جهاز الاستخبارات بتصحيح الوضع. وتشمل الأمثلة الشائعة في تصحيحي الأوضاع دفع تعويضات مالية أو حذف المعلومات التي تم جمعها بصورة

بشأن أجهزة الاستخبارات، بل يمكن أيضا استخدام سلطته لقبول أو رفض ميزانيات من أجل إقناع السلطة التنفيذية و / أو أجهزة الاستخبارات لتغيير السياسات أو الممارسات. وهذا يعني أن نتائج وتوصيات هيئات الإشراف البرلمانية يمكن أن تؤثر في سرعة القرارات وتغيير التشريعات الخاصة بالاستخبارات وميزانياتها. وعلى النقيض لا تملك هيئات الإشراف ذات الخبرة هذه الأدوات المتاحة للتأثير على السلطة التنفيذية وأجهزة الاستخبارات. وفي معظم الحالات، يمكنها فقط رفع النتائج والتوصيات إلى البرلمان والسلطة التنفيذية وأجهزة الاستخبارات.

#### ما هي مزايا هيئات الإشراف ذات الخبرة؟

وبالمقارنة بنظيراتها البرلمانية، تتمتع هيئات الإشراف ذات الخبرة بمزايا كبيرة.

**أولها** أنها عادة ما تكون مستقلة عن التأثيرات السياسية في الوقت الذي يمكن فيه تسييس الهيئات الإشرافية البرلمانية. يميل أعضاء لجان الإشراف البرلمانية أكثر لاستخدام مواقعهم لأغراض سياسية، وهي مشكلة خاصة لأعضاء البرلمان المنتمين للحزب الحاكم إذ قد لا يرغبون في التحقيق في أنشطة معينة من أنشطة أجهزة الاستخبارات التي قد يؤدي كشف نتائجها إلى ضرر أو إحراج للسلطة التنفيذية. وينبع هذا من رغبة النواب حماية حزبهم السياسي، بل وربما طموحاتهم السياسية أيضا. على النقيض من ذلك، يمكن لأعضاء لجان الإشراف البرلمانية من أحزاب المعارضة استغلال منصبهم لمهاجمة الحكومة. على سبيل المثال، قد يسعون إلى بدء التحقيقات لأغراض تضر الحكومة بدلا من القيام بالمهام الإشرافية المنوطة بهم أصلا. ولا شك أن هذه الحقائق تمنع اللجان البرلمانية من أداء مهامهم الإشرافية على أجهزة الاستخبارات بحيادية.

ثانيا، خلافا لأعضاء هيئات الإشراف البرلمانية، يمكن لأعضاء هيئات الإشراف ذات الخبرة التركيز حصرا على الإشراف على أجهزة الاستخبارات، بينما يركز البرلمانيون العاملون في لجان الإشراف على الاستخبارات على أكثر من أجهزة الاستخبارات فقط. على سبيل المثال، تجدهم يشاركون في المناقشات العامة ويعملون في لجان أخرى ويقضون بعض الوقت في الاجتماع بناخبيهم.

ثالثا، عادة ما يظل أعضاء هيئات الإشراف ذات الخبرة في مناصبهم لفترات أطول من أعضاء اللجنة البرلمانية مما يسمح لهم بتطوير معرفتهم وخبرتهم في مجال الاستخبارات. كما يميل الأعضاء العاملون في اللجان البرلمانية إلى ترك

مربع ٩: التعامل مع الشكاوى بواسطة لجنة مراجعة الاستخبارات الأمنية الكندية مراجعة الاستخبارات (SIRC) ١٣

بالإضافة إلى الإشراف على أنشطة أجهزة الاستخبارات الأمنية الكندية، تحقق لجنة مراجعة الاستخبارات الأمنية الكندية في الشكاوى المقدمة ضد جهاز الاستخبارات وتعد جلسات استماع سرية ولها صلاحيات المحكمة من حيث استدعاء الشهود والحصول على أدلة تحت القسم. وتوضح المواد التالية من قانون جهاز الاستخبارات الأمنية الكندية هذه العملية.

**القسم ٤١.**

١. يجوز لأي شخص تقديم شكوى إلى لجنة المراجعة فيما يتعلق بأي إجراء أو شيء قام به جهاز الاستخبارات وتقوم اللجنة وفقا لأحكام الفقرة الفرعية (٢) بالتحقيق في الشكاوى إذا:

- أ. تقدم صاحب الشكاوى بالشكاوى للمدير فيما يتعلق بذلك الإجراء أو الشيء ولم يحصل على رد في غضون فترة من الزمن ترى اللجنة أنها معقولة أو لم يرضى عن الرد
- ب. اقتنعت اللجنة بأن الشكاوى ليست تافهة أو عبثية أو كيدية أو مقدمة بسوء نية.

**القسم ٤٥.**

يجب تقديم الشكاوى بموجب هذا القسم إلى لجنة المراجعة كتابة ما لم تقرر اللجنة خلاف ذلك.

**القسم ٤٨.**

١. التحقيق في كل شكوى بموجب هذا الباب من قبل لجنة المراجعة يجب أن يتم سرا.
٢. في أثناء التحقيق في الشكاوى وفقا لهذا الباب من قبل لجنة المراجعة، يحصل صاحب الشكاوى ونائب الرئيس والمدير المعني على فرصة تقديم تأكيدات للجنة المراجعة وتقديم الأدلة والاستماع إليهم شخصيا أو عن طريق محام، ولكن لا يحق لأي منهم الحصول على أو التعليق على التأكيدات المقدمة للجنة المراجعة من قبل أي شخص آخر.

**القسم ٥٠.**

تتمتع لجنة المراجعة، فيما يتعلق بالتحقيق في أي شكوى بموجب هذا الباب، بسلطة:

١. استدعاء وإنفاذ ممثل الأشخاص أمام اللجنة وإجبارهم على تقديم دليل كتابي أو شفوي تحت اليمين وتجهيز الوثائق والأشياء التي تراها اللجنة لازمة لإجراء تحقيق كامل والنظر في الشكاوى بنفس الطريقة وبنفس القدر من المحكمة العليا للسجلات؛
٢. تأدية القسم
٣. تلقي وقبول الأدلة والمعلومات الأخرى، سواء تحت اليمين أو بموجب شهادة أو خلاف ذلك، حسبما يترأى للجنة، سواء كانت هذه الأدلة أو المعلومات أو ستكون مقبولة لدى المحاكم أم لا.

**القسم ٥٢.**

١. تقوم اللجنة

- أ. حال الانتهاء من التحقيق فيما يتعلق بالشكاوى بموجب المادة ٤١، برفع تقرير إلى الوزير والمدير يتضمن نتائج التحقيق وأية توصيات تراها اللجنة مناسبة
- ب. في نفس وقت أو بعد تقديم التقرير عملا بالفقرة (أ) تقديم تقرير عن نتائج التحقيق في الشكاوى ويجوز لها، إذا رأت ذلك مناسبا، إطلاع صاحب الشكاوى على أي توصيات مشار إليها في تلك الفقرة.

## رزمة - سن التشريعات المتعلقة بالقطاع الأمني

شكوى، كما أنهم لن يقفوا على مدى تأثير هذه الإجراءات على حياتهم. ولما كان الأشخاص غالباً ما يعجزون عن الطعن في هذه الإجراءات، فإن عدداً متزايداً من الدول الديمقراطية تطلب من أجهزة الاستخبارات إبلاغ الأفراد بشأن التدابير السرية التي استخدمت ضدهم. وعادة ما يتم هذا الإبلاغ بعد فترة محددة من الزمن وبشرط ألا يعرض ذلك التحقيقات الجارية للخطر أو يكشف عن المصادر والأساليب المحددة التي تستخدمها أجهزة الاستخبارات (انظر مربع ١٠).

### ما الذي يجعل هيئة نظر الشكاوى فعالة؟

مثلها مثل هيئات الإشراف، تعتبر هيئات نظر الشكاوى مستقلة عن السلطة التنفيذية وأجهزة الاستخبارات، ومن ثم فهي بحاجة إلى سلطة قانونية للوصول إلى جميع المعلومات والمسؤولين وأماكن العمل من أجل التحقيق في الشكاوى.

تتمتع هيئات نظر الشكاوى بمزيد من الفعالية إذا ما تمكنت من إصدار أوامر ملزمة قانوناً لأجهزة الاستخبارات. على سبيل المثال، تمكنهم هذه السلطة من مطالبة أجهزة الاستخبارات بدفع تعويضات للفرد الذي تمت معاملته بطريقة خاطئة من قبل ضباط الاستخبارات. وبالمثل، يمكنها مطالبة أجهزة الاستخبارات بحذف المعلومات التي تم الحصول عليها من خلال الانتهاك غير المشروع لحقوق الفرد.

وحتى تتمكن هيئات نظر الشكاوى من التحلي بالفاعلية في التحقيق وتصحيح انتهاكات حقوق الأفراد، فإنها تحتاج إلى أن تسهل عملية الوصول إليها. فيجب إعلام الجمهور بوجود هيئات لنظر الشكاوى وتمكينه من تقديم الشكاوى عند الضرورة. وتأخذ هذه الهيئات عدة تدابير لضمان إمكانية وصول الجمهور إليها، فهي، أولاً، تعلن عن دورها للجمهور وتقدم معلومات عن كيفية تقديم الشكاوى. على سبيل المثال، تنشئ هذه الهيئات مواقع إلكترونية وتتيح توزيع النشرات في المباني العامة. ثانياً، تتأكد هذه الهيئات من عدم وجود تكلفة لتقديم الشكاوى، وأخيراً، تضمن معاملة الشكاوى سرا. وهذا أمر أساسي لتمكين الأشخاص من الشكاوى دون خوف من انتقام أجهزة الاستخبارات.

غير مشروعة. وتعتمد إمكانية إصدار الهيئة الناظرة في الشكاوى أوامر ملزمة قانوناً لأجهزة الاستخبارات على وضع هذه الهيئة. حيث يمكن للهيئات القضائية إصدار أوامر ملزمة لأجهزة الاستخبارات. وفي معظم الدول، يمكن لهيئات غير قضائية، مثل هيئات الإشراف ذات الخبرة والخبراء ومحققى الشكاوى، إصدار توصيات لأجهزة الاستخبارات. وعلى الرغم من أن أجهزة الاستخبارات غير ملزمة قانوناً بالامتثال لهذه التوصيات، إلا أن الهيئة الناظرة في الشكاوى يمكنها رفع تقرير في هذا الصدد إلى السلطة التنفيذية أو حتى التوجه بها إلى وسائل الإعلام.

### ما هي المؤسسات التي تنظر الشكاوى ضد أجهزة الاستخبارات؟

يمكن للأفراد في معظم الدول تقديم شكاوى ضد أجهزة الاستخبارات لمحقق الشكاوى العام أو مؤسسات حقوق الإنسان و / أو المحاكم العادية. ومع ذلك، وضع عدد متزايد من الدول آليات خاصة لنظر الشكاوى، قضائية وغير قضائية، لتلقي الشكاوى المتعلقة بأجهزة الاستخبارات (انظر مربع ٩). وفي كثير من الأحيان أيضاً، تعمل هيئات الإشراف المتخصصة على أجهزة الاستخبارات بمثابة آليات غير قضائية لنظر الشكاوى.

عادة ما تفضل الدول أن تعهد إلى مؤسسات متخصصة، بدلاً من المحاكم العادية، عملية النظر في الشكاوى المتعلقة بأجهزة الاستخبارات، وذلك لسببين: أولاً، أن موظفي هذه المؤسسات موافق عليهم أمنياً ولديها إجراءات معمول بها للتعامل مع المعلومات السرية على أساس منظم. ثانياً، أن الهيئة المتخصصة القضائية أو غير القضائية يمكنها الإلمام بقضايا الاستخبارات أكثر من المحكمة العادية أو محقق الشكاوى العام أو مؤسسة حقوق الإنسان. ومن الممارسات الجيدة وضع إجراء استئناف ضد القرارات المتخذة من خلال آليات الشكاوى المتخصصة. وعادة، ما تسمح المحاكم العادية بمثل هذا الاستئناف.

### لماذا تخطر بعض الدول الأشخاص حال استخدام صلاحيات خاصة ضدهم؟

أثناء عملية نظر الشكاوى يفترض أن الأفراد يدركون التدابير التي اتخذت ضدهم من قبل أجهزة الاستخبارات، ولكن في كثير من الأحيان لا يكن الأمر كذلك عندما تستخدم أجهزة الاستخبارات صلاحيات خاصة سرا، مثل مراقبة اتصالات شخص ما. وإذا لم يكن الأشخاص على علم بالإجراءات التي اتخذت ضدهم، فلن يمكنهم الطعن عليها من خلال تقديم

مربع ١٠: القانون الألماني بشأن إبلاغ الأفراد بعد استخدام سلطات خاصة ضدهم<sup>١٤</sup>

تطلب العديد من الدول الأوروبية من أجهزة استخباراتها إبلاغ الأشخاص الذين استخدمت ضدهم سلطات خاصة. وفيما يلي مقتطف من القانون الألماني يبين نطاق هذا المطلب. جدير بالذكر أن الإبلاغ لا يحدث في جميع الحالات، ويمكن تأجيله لأسباب محددة. ففي ألمانيا، توجد هيئة إشراف ذات خبرة (لجنة العشر) (G10) تشرف على امتثال أجهزة الاستخبارات لهذه التعليمات.

- يجب إبلاغ صاحب البيانات بالتدابير التقييدية وفقا للقسم ٣ بعد وقف العمل بهذه التدابير.
- يتم حجب هذا الإبلاغ إذا كان ثمة شك أن إبلاغ صاحب البيانات قد يعرض الهدف من التقييد للخطر أو ما دامت هناك أية أضرار قد تلحق بالمصالح العامة للاتحاد أو دولة فيه.
- في حالة استمرار الحجب وفقا للفقرة ٢ اثني عشر شهرا بعد انتهاء هذا الإجراء، فيتعين في هذه الحالة الحصول على موافقة لجنة العشر والتي تحدد أيضا مدة استمرارية الحجب.
- لا يعتبر الإبلاغ ضروريا متى وجدت لجنة العشر بالإجماع ما يلي:
  ١. استمرار سريان أحد الشروط المنصوص عليها في الفقرة ٢ لخمس سنوات بعد انتهاء هذا الإجراء
  ٢. أن يثبت من الناحية العملية أن مثل هذا الشرط سوف يظل ساريا في المستقبل
  ٣. انطباق الشروط المتعلقة بحذف البيانات على كل من الجهة الجامعة للبيانات والمتلقية لها.

## قراءات أخرى

المفوضية الأوروبية من أجل الديمقراطية من خلال القانون، (لجنة فينيسيا)، تقرير عن الإشراف الديمقراطي على الأجهزة الأمنية، التي اعتمدهت لجنة فينيسيا في جلستها العامة رقم ٧١، CDL-AD(٢٠٠٧)٠١٦ (فينيسيا، ٢-١ يونيو ٢٠٠٧).

[http://www.venice.coe.int/docs/2007/CDL-AD\(2007\)016-e.asp](http://www.venice.coe.int/docs/2007/CDL-AD(2007)016-e.asp)

اللجنة الدولية للحقوقيين، مجموعة الحقوقيين البارزين، إجراء تسريع تقييم الأضرار، تقرير مجموعة الحقوقيين البارزين حول الإرهاب ومكافحة الإرهاب وحقوق الإنسان (جنيف: محكمة العدل الدولية، ٢٠٠٩).

<http://ejp.icj.org/IMG/EJP-Report.pdf>

لجنة المراجعة الوزارية بشأن الاستخبارات في جنوب أفريقيا، الاستخبارات في الديمقراطية الدستورية، التقرير النهائي إلى وزير الاستخبارات، (بريتوريا: ٢٠٠٨).

[http://www.ssr-online.org/edocs/review\\_commission\\_final\\_report20080910.doc](http://www.ssr-online.org/edocs/review_commission_final_report20080910.doc)

مفوض الأمم المتحدة السامي لحقوق الإنسان، حقوق الإنسان والإرهاب ومكافحة الإرهاب، صحيفة وقائع رقم ٣٢، يوليو ٢٠٠٨.

<http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf>

مجلس حقوق الإنسان التابع للأمم المتحدة، مجموعة من الممارسات الجيدة بشأن الأطر المؤسسية والقانونية والتدابير التي تضمن احترام حقوق الإنسان من قبل أجهزة الاستخبارات في سياق مكافحة الإرهاب، بما في ذلك الإشراف عليها، HRC/A/١٤/٤٦، ١٧ مايو ٢٠١٠.

<http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf>

بورن هانز و «ايان ليه»، إخضاع الاستخبارات للمساءلة، (مركز جنيف للرقابة الديمقراطية على القوات المسلحة / البرلمان النرويجي: أوسلو، ٢٠٠٥). متوفر باللغات التالية: الألبانية والعربية والبلغارية والكرواتية والداري والإنجليزية والجورجية والاندونيسية والمقدونية والروسية والصربية والباشتو والإسبانية والتركية والأوكرانية.

<http://www.dcaf.ch/publications/kms/details.cfm?id=18718&nav1=5>

مجموعة أدوات مركز جنيف للرقابة الديمقراطية على القوات المسلحة، تشريعات قطاع الأمن، نموذج تشريعات الاستخبارات - الأرجنتين، قانون الاستخبارات الوطنية (والقرارات ذات الصلة)، ٢٠٠١.

مجموعة أدوات مركز جنيف للرقابة الديمقراطية على القوات المسلحة، تشريعات قطاع الأمن، نموذج تشريعات الاستخبارات - كندا، قانون جهاز الاستخبارات الكندية، ١٩٨٥.

مجموعة أدوات مركز جنيف للرقابة الديمقراطية على القوات المسلحة، تشريعات قطاع الأمن، نموذج تشريعات الاستخبارات - هولندا، قانون أجهزة الأمن والاستخبارات، ٢٠٠٢.

مجموعة أدوات مركز جنيف للرقابة الديمقراطية على القوات المسلحة، تشريعات قطاع الأمن، نموذج تشريعات الاستخبارات - القوانين البرازيلية بشأن أجهزة الاستخبارات.

لجنة التحقيق بشأن بعض أنشطة الشرطة الملكية الكندية، التقرير الثاني (أوتاوا: مكتب المجلس الملكي الخاص، ١٩٨١).

<http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm>

## ملاحظات ختامية

- ١- مقتطفات من الأقسام ١٢-١٥، وكالة الاستخبارات الكندية قانون ١٩٨٤، والمادة ١ من قانون نظام الاستخبارات الأمنية لجمهورية كرواتيا، ٢٠٠٦ والمادة ٦ من قانون الأجهزة الأمنية والاستخبارات ٢٠٠٢.
- ٢- مقتطفات من دستور جمهورية جنوب أفريقيا، ١٩٩٦، ١٩٨٨، ١٩٩٠-٢٠٩-٢١٠.
- ٣- العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR). ١٦ ديسمبر ١٩٦٦، دخل حيز النفاذ ٢٣ مارس ١٩٧٦، والمادة (٤)؛ لجنة الأمم المتحدة لحقوق الإنسان، التعليق العام رقم ٢٩، حالات الطوارئ (المادة ٤)، وثيقة الأمم المتحدة. CCPR/C/21/Rev.1/Add.11 (٢٠٠١).
- ٤- اتفاقيات جنيف ١-٤، ١٢ أغسطس ١٩٤٩، دخلت حيز النفاذ ٢١ أكتوبر ١٩٥٠.
- ٥- العهد، المادة ٤؛ لجنة الأمم المتحدة لحقوق الإنسان، التعليق العام رقم ٢٩، حالات الطوارئ (المادة ٤)؛ وثيقة الأمم المتحدة. CCPR/C/21/Rev.1/Add.11 (٢٠٠١). مبادئ سيراكوزا بشأن الحد والانتقاص من الأحكام الواردة في العهد الدولي الخاص بالحقوق المدنية والسياسية، المرفق، وثيقة الأمم المتحدة E/CN.4/1984/4 (١٩٨٤)؛
- ٦- مقتطفات من قانون جهاز الاستخبارات الأمنية الكندية، ١٩٨٤، القسم ٢١.
- ٧- مقتطفات من القانون الاتحادي لحماية الدستور، ١٩٩٠، الأقسام ١٠ و ١٢ و ٣، قانون لجنة العشر، ٢٠٠١. القسم ١٥.
- ٨- مقتطفات من القانون الاتحادي الألماني لحماية الدستور، ١٩٩٠، القسم ١٥.
- ٩- مقتطفات من قانون نظام الاستخبارات الأمنية لجمهورية كرواتيا، ٢٠٠٦.
- ١٠- العهد الدولي الخاص بالحقوق المدنية والسياسية؛ مجموعة المبادئ المتعلقة بحماية جميع الأشخاص الذين يتعرضون لأي شكل من أشكال الاحتجاز أو السجن، مرفق قرار الجمعية العامة A/RES/43/173، ٩ ديسمبر ١٩٨٨، واتفاقية مناهضة التعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة ٣٩/٤٦ في ١٠ ديسمبر ١٩٨٤ ودخلت حيز النفاذ في ٢٦ يونيو ١٩٨٧.
- ١١- المبادئ الأساسية بشأن استخدام القوة والأسلحة النارية من جانب الموظفين المكلفين بإنفاذ القوانين التي اعتمدها مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة المجرمين، هافانا، كوبا، ٢٧ أغسطس - ٧ سبتمبر ١٩٩٠؛ مدونة قواعد سلوك الموظفين المكلفين بإنفاذ القوانين، اعتمدت بموجب قرار الجمعية العامة ٣٤/١٦٩ المؤرخ ١٧ ديسمبر ١٩٧٩؛ العهد الدولي الخاص بالحقوق المدنية والسياسية، دخل حيز النفاذ ٢٣ مارس ١٩٧٦.
- ١٢- استمدت هذه المادة من قانون أجهزة الاستخبارات البريطانية ١٩٩٤؛ وزارة العدل بالمملكة المتحدة، الحكم في بريطانيا - التجديد الدستوري، (لندن: HMSO، ٢٠٠٨)؛ بلجيكا - القانون الحاكم لمراجعة أجهزة الشرطة والاستخبارات ووحدة التنسيق لتقييم التهديد، ١٩٩١؛ قانون جهاز الاستخبارات الكندية، ١٩٨٤، جنوب أفريقيا - قانون الإشراف على أجهزة الاستخبارات، قانون ٤٠ لسنة ١٩٩٤، ومواقع الانترنت للجنة مراجعة الاستخبارات الأمنية (www.sirc-csars.gc.ca)، اللجنة البلجيكية الدائمة لمراجعة وكالات الاستخبارات (www.comiteri.be).
- ١٣- مقتطفات من قانون الاستخبارات الأمنية الكندي، ١٩٨٤، وموقع الانترنت للجنة مراجعة الاستخبارات الأمنية (SIRC): www.sirc - csars.gc.ca.
- ١٤- مقتطفات من قانون لجنة العشر، ٢٠٠١، القسم ١٢.







مركز جنيف للرقابة الديمقراطية على القوات المسلحة  
شارع المعارف ٣٤  
رام الله / البيرة  
الضفة الغربية  
فلسطين

هاتف: +٩٧٢ (٢) ٢٩٥ ٦٢٩٧  
فاكس: +٩٧٢ (٢) ٢٩٥ ٦٢٩٥

مركز جنيف للرقابة الديمقراطية على القوات المسلحة  
مركز جيفنور - بلوك C - الطابق السادس  
شارع كليمنسو  
بيروت  
لبنان

هاتف: +٩٦١ (٠) ١٧٣٨ ٤٠١  
فاكس: +٩٦١ (٠) ١٧٣٨ ٤٠٢

#### **DCAF Head Office, Geneva**

By Post:

Geneva Centre for the Democratic Control of Armed Forces (DCAF)  
P.O.Box 1360  
CH-1211 Geneva 1  
Switzerland

For Visitors:

Geneva Centre for the Democratic Control of Armed Forces (DCAF)  
Rue de Chantepoulet 11  
CH-1201 Geneva 1  
Switzerland

Tel: +41 (0) 22 741 77 00  
Fax: +41 (0) 22 741 77 05

#### **DCAF Ramallah**

Al-Maaref Street 34  
Ramallah / Al-Bireh  
West Bank  
Palestine

Tel: +972 (2) 295 6297  
Fax: +972 (2) 295 6295

#### **DCAF Beirut**

Gefinor Center - Block C - 6<sup>th</sup> Floor  
Clemenceau Street  
Beirut  
Lebanon

Tel: +961 (0) 1 738 401  
Fax: +961 (0) 1 738 402

[www.dcaf.ch](http://www.dcaf.ch)









## Endnotes

1. Extracts from Sections 12-15, *Canadian Security Intelligence Service Act*, 1984; Article 1, Act on the Security Intelligence System of the Republic of Croatia, 2006; and Article 6 of The Netherlands Intelligence and Security Services Act 2002.
2. Extracts from the Constitution of the Republic of South Africa, 1996, 198 -199, 209-210.
3. International Covenant on Civil and Political Rights (ICCPR), 16 December 1966, entry into force 23 March 1976, Article 4; UN Human Rights Committee, General Comment 29, States of Emergency (article 4), U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001).
4. Geneva Conventions 1-4, 12 August 1949, entry into force 21 October 1950.
5. ICCPR, Article 4; United Nations Human Rights Committee, General Comment 29, States of Emergency (article 4); U.N. Doc. CCPR/C/21/Rev.1/Add.11 (2001). Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4 (1984);
6. Extracts from the Canadian Security Intelligence Service Act, 1984, Section 21.
7. Extracts from Federal Act on Protection of the Constitution, 1990, Sections 10, 12, 3; and G10 Act, 2001, Section 15.
8. Extracts from German Federal Act on the Protection of the Constitution, 1990, Section 15.
9. Extracts from the Act on the Security Intelligence System of the Republic of Croatia, 2006
10. International Covenant on Civil and Political Rights; Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment, Annex to General Assembly Resolution, A/RES/43/173, 9 December 1988; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, Adopted and opened for signature, ratification and accession by General Assembly resolution 39/46 of 10 December 1984, entry into force 26 June 1987.
11. Basic Principles on the Use of Force and Firearms by Law Enforcement Officials. Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, 27 August to 7 September 1990; Code of Conduct for Law Enforcement Officials, Adopted by General Assembly resolution 34/169 of 17 December 1979; International Covenant on Civil and Political Rights, entry into force 23 March 1976.
12. This material was drawn from UK Intelligence Services Act 1994; UK Ministry of Justice, *The Governance of Britain – Constitutional Renewal*, (London: HMSO, 2008); Belgium – Act Governing Review of the Police and Intelligence Services and the Coordination Unit for Threat Assessment, 1991; Canadian Security Intelligence Service Act, 1984; South Africa – Intelligence Services Oversight Act, Act 40, 1994; and the websites of the Security Intelligence Review Committee ([www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)), and the Belgian Standing Intelligence Agencies Review Committee ([www.comiteri.be](http://www.comiteri.be)).
13. Extracts from the Canadian Security Intelligence Service Act, 1984 ; and the website of the Security Intelligence Review Committee (SIRC): [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca).
14. Extracts from the G10 Act, 2001, Section 12.

## Further Reading

Born, Hans and Ian Leigh, *Making Intelligence Accountable*, (DCAF/Norwegian Parliament: Oslo, 2005). Available in the following languages: Albanian, Arabic, Bulgarian, Croatian, Dari, English, Georgian, Indonesian, Macedonian, Russian, Serbian, Pashto, Spanish, Turkish, Ukrainian.

<http://www.dcaf.ch/publications/kms/details.cfm?id=18718&nav1=5>

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Argentina, National Intelligence Law (and associated decrees), 2001.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Canada, Canadian Security Intelligence Service Act, 1985.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – The Netherlands, Intelligence and Security Services Act 2002.

DCAF Toolkit, Legislating for the security sector, Intelligence Legislation Model – Brazilian laws on the intelligence services.

Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Second Report*, (Ottawa: Privy Council Office, 1981).

<http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-eng.htm>

European Commission for Democracy Through the Law, (Venice Commission), *Report on the democratic oversight of the security services*, adopted by the Venice Commission at its 71st Plenary Session, CDL-AD(2007)016 (Venice, 1-2 June 2007).

[http://www.venice.coe.int/docs/2007/CDL-AD\(2007\)016-e.asp](http://www.venice.coe.int/docs/2007/CDL-AD(2007)016-e.asp)

International Commission of Jurists, Eminent Jurists Panel, *Assessing Damage Urging Action, Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights* (Geneva: ICJ, 2009).

<http://ejp.icj.org/IMG/EJP-Report.pdf>

Ministerial Review Commission on Intelligence in South Africa, *Intelligence in a Constitutional Democracy*, Final Report to the Minister for Intelligence Services, (Pretoria: 2008).

[http://www.ssronline.org/edocs/review\\_commission\\_final\\_report20080910.doc](http://www.ssronline.org/edocs/review_commission_final_report20080910.doc)

UN High Commissioner for Human Rights, *Human Rights, Terrorism and Counter-Terrorism*, Fact sheet No. 32, July 2008.

<http://www.ohchr.org/Documents/Publications/Factsheet32EN.pdf>

UN Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, A/HRC/14/46, 17 May 2010.

<http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf>

### **What makes a complaints-handling body effective?**

Like oversight bodies, complaints-handling bodies are independent from both the executive and the intelligence services. They need the legal power to access all information, officials and premises in order to investigate a complaint.

Complaints-handling bodies are more effective if they can issue orders that are legally binding on intelligence services. For example, this power enables them to require intelligence services to pay compensation to an individual who was wrongly treated by an intelligence officer. Similarly, they could require intelligence services to delete information which was acquired through the unlawful infringement of an individual's rights.

In order for complaints-handling bodies to be effective in investigating and remedying violations of individuals' rights, they need to be easily accessible. Members of the public must be aware that complaints-handling bodies exist and be able to file a complaint if necessary. These bodies take several measures to ensure that they are accessible. First, they advertise their role to the public and provide information on how complaints can be filed. For example, they establish websites and make leaflets available in public buildings. Second, they make sure that there is no cost to submit a complaint. Finally, they guarantee that complaints will be treated confidentially. This is essential to enable people to complain without fear of reprisals from intelligence services.

### Which institutions handle complaints about the intelligence services?

In most states individuals can submit complaints about intelligence services to general ombudsman or human rights institutions and/or the ordinary courts. However, an increasing number of states have established special complaint-handling mechanisms, both judicial and non-judicial, to receive complaints relating to the intelligence services (see Box 9). Specialised intelligence oversight bodies often also act as non-judicial complaints-handling mechanisms.

States usually prefer to entrust specialised institutions, rather than the regular courts, with the handling of complaints related to their intelligence services for two reasons. First, such bodies can have security-cleared staff and they have procedures in place to handle classified information on a regular basis. Second, a specialised judicial or non-judicial body can develop knowledge of intelligence issues that ordinary courts or a general ombudsman or human rights institution may not have.

It is good practice to establish an appeal procedure against the decisions of specialised complaint mechanisms. Usually, ordinary courts process such appeals.

### Why do some states notify people when special powers have been used against them?

A complaints-handling process assumes that individuals are aware of measures that have been taken against them by intelligence services. This is often not the case when intelligence services use special powers secretly, such as monitoring a person's communications. If people have no knowledge of actions taken against them they cannot challenge those actions by filing a complaint. Nor do they know how such actions will affect their lives. Because individuals often cannot challenge such actions, an increasing number of democratic states require intelligence services to inform individuals about secret measures that have been used against them. This notification usually takes place after a fixed period of time and is given only when it would not jeopardise ongoing investigations or reveal the specific sources and methods used by the intelligence services (see Box 10).

#### Box 10: German law on notifying individuals after special powers have been used against them<sup>14</sup>

Many European states require their intelligence services to inform persons against whom they have used special powers. The following extract from German law shows the scope of this requirement. Notification does not take place in all cases, and may be postponed on specific grounds. In Germany, an expert oversight body (G10 Commission) oversees the intelligence services' compliance with these regulations.

- The data subject shall be informed of restrictive measures pursuant to Section 3 after their discontinuation.
- Such notification shall be withheld as long as it cannot be ruled out that informing the data subject might jeopardise the purpose of the restriction or as long as any general disadvantages to the interests of the Federation or of a Federal State are foreseeable.
- Where such notification continues to be withheld pursuant to sentence 2 twelve months after termination of the measure, its continued deferment shall require the approval of the G10 Commission. The G10 Commission shall determine the duration of the continued deferment.
- No notification shall be necessary where the G10 Commission has unanimously found that:
  1. one of the conditions stipulated in sentence 2 continues to apply five years after termination of the measure,
  2. it is practically certain that such a condition will continue to apply in the future
  3. the conditions pertaining to erasure apply both at the collecting agency and at the receiving agency.

**Box 9: Complaints-handling by Canada’s Security Intelligence Review Committee (SIRC)<sup>13</sup>**

In addition to overseeing the activities of the Canadian Security Intelligence Service, the SIRC investigates complaints made about the intelligence service. It holds in camera hearings and has the powers of a court to summon witnesses and receive evidence under oath. The following articles from the Canadian Security Intelligence System (CSIS) Act outline this process.

**Section 41.**

1. Any person may make a complaint to the Review Committee with respect to any act or thing done by the (intelligence) Service and the Committee shall, subject to subsection (2), investigate the complaint if:
  - a. the complainant has made a complaint to the Director with respect to that act or thing and the complainant has not received a response within such period of time as the Committee considers reasonable or is dissatisfied with the response given; and
  - b. the Committee is satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

**Section 45.**

A complaint under this Part shall be made to the Review Committee in writing unless the Committee authorizes otherwise.

**Section 48.**

1. Every investigation of a complaint under this Part by the Review Committee shall be conducted in private.
2. In the course of an investigation of a complaint under this Part by the Review Committee, the complainant, deputy head concerned and the Director shall be given an opportunity to make representations to the Review Committee, to present evidence and to be heard personally or by counsel, but no one is entitled as of right to be present during, to have access to or to comment on representations made to the Review Committee by any other person.

**Section 50.**

The Review Committee has, in relation to the investigation of any complaint under this Part, power:

1. to summon and enforce the appearance of persons before the Committee and to compel them to give oral or written evidence on oath and to produce such documents and things as the Committee deems requisite to the full investigation and consideration of the complaint in the same manner and to the same extent as a superior court of record;
2. to administer oaths; and
3. to receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Committee sees fit, whether or not that evidence or information is or would be admissible in a court of law.

**Section 52.**

1. The Review Committee shall,
  - a. on completion of an investigation in relation to a complaint under section 41, provide the Minister and the Director with a report containing the findings of the investigation and any recommendations that the Committee considers appropriate; and
  - b. at the same time as or after a report is provided pursuant to paragraph (a), report the findings of the investigation to the complainant and may, if it thinks fit, report to the complainant any recommendations referred to in that paragraph.

belonging to the governing party. They may be unwilling to investigate particular activities of the intelligence services that could reveal findings that are damaging or embarrassing for the executive. This stems from the desire of MPs to protect their own political party, and potentially their own political ambitions. By contrast, members of parliamentary oversight committees from opposition parties may exploit their position to attack the government. For example, they may attempt to launch investigations for the purposes of damaging the government rather than to genuinely carry out their oversight mandate. These realities inhibit parliamentary committees from fully conducting impartial oversight of intelligence services.

Second, unlike parliamentarians, members of expert oversight bodies can focus exclusively on overseeing the intelligence services. Parliamentarians serving on intelligence oversight committees focus on more than just intelligence services. For example, they take part in plenary debates, serve on other committees and spend time meeting with their constituents.

Third, members of expert oversight bodies usually remain in office for longer periods than parliamentary committee members. Longer periods in the job enable members of expert oversight bodies to develop knowledge of and expertise in the intelligence field. Members serving on parliamentary committees tend to leave more frequently and do not generally develop the same level of knowledge and expertise.

Finally, since members of expert oversight bodies are generally less likely to be influenced by politics, they are probably also less likely to leak sensitive information for political purposes. Also, there are often greater numbers of parliamentarians serving on committees who have access to classified information compared to members of expert oversight bodies. Thus, parliamentary committees are more likely to misuse sensitive information for political reasons such as leaking information to discredit political opponents. Intelligence services place much value on the security of their information. In many states intelligence services generally distrust parliament and may fear that members of parliamentary oversight committees will leak classified information.

## Complaints about intelligence services

### How can the public complain about intelligence services?

In democratic societies, individuals have a right to complain about any action taken against them by a public institution, including intelligence services. Any person can challenge an action that an intelligence service might have taken against them, including arrest and detention, the search of their home or the interception of their communications.

Persons who believe they have been unfairly or unlawfully treated by intelligence services file their complaints with an independent body. (See Box 9 for an example of how complaints about intelligence services can be handled). This complaints-handling body is normally a court or a non-judicial body such as an ombudsman or expert intelligence oversight body. This body must first assess whether the intelligence service took action against the person concerned and, if so, whether it used its powers in compliance with the law.

If the complaints-handling body finds a complaint to be valid, it may request or order the intelligence service to remedy the situation. Common examples of remedies include the payment of financial compensation or the deletion of information collected unlawfully. Whether or not a complaints-handling body can issue legally binding orders to the intelligence services depends on its status. Judicial bodies can issue binding orders which intelligence services must comply with. In most states, non-judicial bodies, such as expert oversight bodies and ombudsmen, can issue recommendations to intelligence services. They are not legally obliged to comply with such recommendations but the complaints-handling body may be able to report non-compliance to the executive, and could even go to the media.

recommendations in reports.

In many democratic states, intelligence oversight bodies also have budgetary independence. This means that they can request their own funding from parliament and manage their own budgets. Because they are financially independent, other organisations (e.g. the executive, intelligence services) cannot influence their decisions by threatening them with funding cuts.

### How can the independence of members of oversight bodies be ensured?

The independence of an oversight body is only guaranteed if its members and staff remain independent. This implies that they do not misuse their positions for personal gain or for advancing the interests of others. Thus, democratic societies adopt laws to make sure that individuals appointed to oversight bodies are and remain independent.

Usually, the law regulates the selection and appointment of members of oversight bodies. In many states parliament appoints members of oversight bodies. This means that overseers are chosen by an institution that is independent from those being overseen. This is necessary to ensure the independence of persons who serve on oversight bodies. In a few states, the executive is responsible for appointing members of oversight bodies but its choices need the approval of parliament and in some cases the judiciary.

The fact that members of oversight bodies are appointed for fixed terms of office gives them additional independence and protects them against external pressure. As terms of office are defined by law, politicians cannot arbitrarily dismiss them. Dismissals are only possible, if the person has committed a serious offence or failed to perform his or her duties. In some countries, the law does not allow members of oversight bodies to serve a second term. By limiting mandates to one term, legislators have sought to prevent members of oversight bodies from misusing their position with the goal of influencing decisions to re-appoint them.

As an additional measure for ensuring independence, the law may prohibit serving members of oversight bodies from holding other positions. For obvious reasons, members

of oversight bodies cannot serve in intelligence services. But the law may also prohibit overseers from holding membership of a political party or engaging in commercial activities. This helps to prevent a possible conflict of interests.

### What are the advantages of parliamentary oversight bodies?

Parliamentary oversight bodies have two main advantages when compared with expert ones. First, and most importantly, parliamentary oversight has more “democratic legitimacy” because it is carried out by elected individuals; those who oversee intelligence services have a direct link with the public. By contrast, members of expert oversight bodies have only an indirect legitimacy, because they are normally selected by either parliament or the executive.

Second, parliamentary oversight bodies are better placed to directly influence the policies and activities of the executive and intelligence services. Parliament has two main tools at its disposal in this regard: it may be able to pass or amend legislation on the intelligence services; it can also use its power to approve or reject budgets in order to persuade the executive and/or the intelligence services to change policies or practices. This means that the findings and recommendations of parliamentary oversight bodies can quickly influence decisions and force change on intelligence legislation and budgets. Expert oversight bodies do not have these instruments available to influence the executive and the intelligence services. In most cases, they can only issue findings and recommendations to parliament, the executive, and the intelligence services.

### What are the advantages of expert oversight bodies?

In comparison to their parliamentary counterparts, expert oversight bodies offer significant advantages.

First, expert oversight bodies are usually independent from political influences while parliamentary oversight can become politicised. Members of parliamentary oversight committees are more likely to use their positions for political purposes. This is a particular problem for members of parliament

members of oversight bodies and their staff must obtain security clearances, before being allowed access to classified information. This means that they are screened to ensure that they can be trusted to have access to classified information. Additionally, overseers may be required to sign special agreements stating they will not disclose classified information.

Third, oversight bodies need to take measures to prevent staff from disclosing classified information. They usually adopt policies prohibiting members and staffers from taking classified information off the premises. Also, special security measures may apply to protect electronic and hard copy documents containing sensitive information.

Finally, laws on the protection of personal data apply to oversight bodies, as they do to any other public institution. The law requires oversight bodies to keep personal data confidential. Oversight bodies may only disclose them with the consent of the person concerned, and in accordance with other specific criteria set out in law.

### **Why is the relationship between intelligence services and oversight bodies important?**

Oversight bodies generally seek to develop a constructive relationship with the intelligence services they monitor. This is because it is very difficult for overseers to monitor intelligence services properly without their cooperation. Overseers rely on intelligence services to facilitate their access to the information needed. Oversight bodies can gain the trust of intelligence services by treating classified information with care and by keeping them informed about oversight activities.

Intelligence services benefit too from a constructive working relationship with oversight bodies. The reports of oversight bodies can foster their legitimacy and build public confidence in their work. In some cases, oversight reports can also help intelligence services to make a case for additional financial or human resources. Additionally, if allegations are made about intelligence services, an investigation by an oversight body can sometimes help re-establish public confidence in them. Oversight bodies can also play a role in protecting intelligence services

against potential misuse by the executive. Intelligence officials can report inappropriate or illegal orders they receive to the oversight body. Considering these benefits, it is generally in the interest of intelligence services to cooperate with oversight bodies.

While the working relationship needs to be constructive, it should not be too close. The public will only perceive oversight bodies as independent, and therefore effective, if they maintain a certain distance from the intelligence services.

### **How do democratic societies ensure the independence of intelligence oversight bodies?**

Parliamentary and expert oversight bodies are independent organisations. They cannot be part of the executive or the intelligence services, as they must oversee those who collect and use intelligence information.

Democratic states adopt laws giving intelligence oversight bodies an independent legal identity. The intent of these laws is to protect their organisational and operational independence. These laws authorise oversight bodies to pursue their own activities without interference from the executive or intelligence services. For example, they select the cases or themes they will investigate and decide how they will conduct investigations. The independent legal identity of oversight bodies means that they cannot take any instructions from the executive or the intelligence services.

Oversight bodies can also decide independently which information they need to access from the intelligence services. Legally guaranteed access to information ensures that neither the intelligence services nor the executive may control the work of oversight bodies by restricting their access to information. In some instances, oversight bodies may rely on the courts to require intelligence services to give them access to relevant information.

Oversight bodies can also make independent decisions related to reporting. In practice, overseers consult intelligence services and the executive before publishing a report. However, the executive and intelligence services have no legal recourse to stop oversight bodies from publishing their independent findings and

Finally, some parliamentary and expert oversight bodies investigate specific complaints made by individuals (see pages 43-46). By investigating specific complaints, overseers get an insight into broader problems in the work of intelligence services. Oversight bodies look for patterns in the complaints they receive; this can serve as the basis for further investigations.

### How do oversight bodies report on their activities?

Generally, the law requires oversight bodies to issue annual public reports on their activities. These reports usually include information about their current membership, investigations carried out, their findings, finances, and recommendations. The recommendations advise the intelligence services and the executive on how they can improve their accountability, transparency, legality and effectiveness.

Oversight bodies may provide additional reports in a given year. They produce special reports describing investigations they have conducted on specific events or general themes. Oversight bodies usually produce two versions of their reports. They produce one version for the executive and the intelligence services which may contain classified information and a second version for the public which generally does not contain classified information. Oversight bodies consult with the executive and intelligence services before releasing public reports. This consultation gives the executive and intelligence services the chance to share any concerns they may have regarding the inclusion of sensitive information in the report.

### Why are public reports important?

First, public reporting informs society about intelligence services' activities while also promoting public understanding and confidence in the intelligence oversight body.

Second, overseers use their reports to try to bring about change within the intelligence services, to executive policies on intelligence, or to the legislation that regulates intelligence activities. The reports of oversight bodies often contain recommendations on how to improve particular policies and practices. Overseers can follow up on such recommendations in subsequent years to

hold the intelligence services and the executive to account for addressing problems previously identified in their organisation.

### Is there a conflict between the right to know and the need to keep information secret?

In order to monitor intelligence services, parliamentary and expert oversight bodies require detailed information about their activities. In most democratic states they have a legal right to access all information relevant to their work. On the other side, intelligence services need to protect information, which, if made public, could harm ongoing investigations or expose their methods and sources used for collecting information. The public disclosure of such information could also be harmful to national security. Intelligence services are often uneasy about overseers having full access to their information because they are afraid that classified information might be leaked.

Besides, many intelligence services are concerned that overseers might undermine their confidentiality obligations regarding personal data. The law requires intelligence services and their personnel to treat personal data confidentially, and restricts the sharing of such information.

Given these competing demands on information held by intelligence services, there is a potential for conflict between intelligence services and overseers regarding access to information. However, several measures can prevent such conflicts (see below).

### How can the information needs of oversight bodies and intelligence services be reconciled?

Special measures help make sure that oversight bodies handle classified information appropriately. These measures help to reassure intelligence services that overseers will not leak classified information.

First, parliamentary and expert oversight bodies hold most of their meetings in private. The content of these meetings is not made public.

Second, it is common practice in democratic states for the law to make the disclosure of classified information a criminal offence. In many states,

Third, oversight bodies have the authority to call upon ministers and officials responsible for intelligence services to give answers to their questions related to intelligence work. In many states, these individuals must testify under oath to the oversight body.

Finally, oversight bodies are free to visit the premises of intelligence services. Such visits may be arranged in advance with intelligence services, or unannounced.

### Why do oversight bodies need financial and human resources?

In addition to legal powers, oversight bodies require financial and human resources to carry out their role effectively. Oversight bodies need sufficient funding to hire permanent staff and to engage the services of specific experts when needed. They also need funding to buy equipment, such as computers. Given that they handle highly sensitive information, they need highly sophisticated computer equipment and technical experts to set up security systems.

Oversight bodies hire permanent staffers who perform roles that are essential to their organisation. Staffers do much of the day-to-day work of oversight bodies. Their tasks include preparing for inspections, conducting analyses of intelligence activities and reporting on the oversight body's investigations. While the members of both parliamentary and expert oversight bodies may change, staffers often remain with the organisation for longer periods than members. Thus, they are able to provide important continuity of activities as well as provide the organisation with "institutional memory". Their long tenures also give them developed knowledge and expertise in many aspects of intelligence work.

Parliamentary oversight bodies usually select staffers who are already employed by parliament. Expert oversight bodies usually hire their staff from outside of government. In both cases staffers must receive security clearances to ensure they can be trusted to handle sensitive information related to intelligence services.

Overseeing intelligence services requires expertise and knowledge of complex practices that very few people outside of the

intelligence community possess. Therefore, in some cases they need to hire intelligence experts to help them do investigations and effectively deal with complex issues related to intelligence work. Likewise, they often need IT and telecommunications experts with intelligence backgrounds to help them gain a better understanding of the complex electronic techniques that are used by intelligence services.

### How do overseers monitor intelligence services?

Parliamentary and expert oversight bodies use many different methods to monitor the activities of intelligence services. The methods used depend on the oversight body's mandate and legal powers.

First, they read classified and unclassified reports produced by intelligence services. Reports give them useful information relating to all aspects of intelligence work. This stimulates further questions which may lead to a better understanding of internal processes.

Second, they do random sampling of information intelligence services have processed or stored. Random sampling can be done during regular inspections or through unannounced visits. For example, if they wish to assess whether intelligence services are using personal data in accordance with the law, they randomly select a number of individual files and check to see if these samples meet the requirements.

Third, they conduct thematic investigations to carefully examine a specific area of intelligence work. These investigations usually focus on broad areas rather than specific events or activities. Oversight bodies often select themes based on particular concerns. These may have been brought to their attention by the public or governmental and non-governmental entities, often as a follow-up to previous inquiries or inspections.

Fourth, they also conduct investigations into specific events or allegations concerning intelligence services. They initiate investigations of specific incidents on their own or do them when the executive and/or parliament have inquiries. These investigations examine all relevant information held by intelligence services relating to specific events and allegations.

## **An in-depth study of parliamentary and expert intelligence oversight bodies**

This section examines the role played by specialised parliamentary oversight committees and expert intelligence oversight bodies. It addresses questions about their mandates; powers; resources; handling of classified information; relationships with intelligence services; independence; reporting functions; and finally, the advantages and disadvantages of both parliamentary and expert oversight bodies.

### **Which aspects of intelligence services' work are overseen by parliamentary and/or expert oversight bodies?**

Parliamentary committees and/or expert oversight bodies oversee all aspects of intelligence services (see Table 2 for examples). They focus on four areas:

#### **1. Oversight of the legality of operations and policy**

Overseers evaluate whether existing policies and all aspects of ongoing intelligence operations comply with national law and international standards. They also assess whether completed intelligence operations and activities have met legal requirements. Finally, overseers review plans for future intelligence operations and determine whether those activities will comply with existing laws, regulations and international standards.

#### **2. Oversight of effectiveness of operations**

Overseers monitor the effectiveness of intelligence operations. They determine whether intelligence services are effectively performing their functions, activities and tasks in accordance with the law and the executive's policies and priorities.

#### **3. Oversight of administrative practices**

Overseers monitor intelligence services' administrative practices. They examine human resources policies and management practices among other things.

#### **4. Oversight of financial management**

Overseers monitor intelligence services' internal financial activities including their budgeting and expenditures.

In some systems states establish only one parliamentary or expert oversight body to monitor and evaluate intelligence services' activities. However, more commonly, states engage more than one oversight body to monitor all the aspects of intelligence work. For example, a state may assign a parliamentary oversight committee the responsibility for monitoring the effectiveness of intelligence activities, and give an expert oversight body the responsibility for monitoring the legality of their activities. Regardless of the precise composition of the system of oversight, democratic states ensure that all aspects of intelligence services' activities are overseen by one or more external bodies.

### **What legal powers do oversight bodies have?**

Democratic societies ensure that parliamentary and expert oversight bodies' roles, mandates and powers are based on legislation (see Table 2 for examples). The law requires the executive and intelligence services to cooperate with oversight bodies; this is essential for performing their role.

The law gives oversight bodies the powers needed for scrutinising the work of intelligence services, which is necessary for holding them accountable for their actions.

First, the law gives oversight bodies the power to act independently and to initiate their own investigations without the need to obtain prior permission from the executive or the intelligence services.

Second, the law gives oversight bodies full access to all information relevant for their work, including the secret files held by intelligence services. Access to this information is essential for determining whether, among other things, intelligence services are operating effectively and in compliance with the law. An intelligence officer's failure to comply with an oversight body's request for information may be considered a criminal offence under the law. In many states, an oversight body may call upon law enforcement authorities to compel individuals to comply with their requests for information.

	Belgium	Canada	South Africa	United Kingdom
Access to classified information	Access to all information they deem necessary; Intelligence services must, on their own initiative, supply the committee with all internal rules & directives.	Unlimited access to all information necessary for the performance of its duties and functions.	Some limitations on access to information held by intelligence services; the names of agents and/ or sources can be withheld from the committee.	The responsible minister can limit the committee's access to sensitive information which could reveal details of operations, or sources and methods of the intelligence services.
Triggers for investigations	Own initiative; A complaint; At request of parliament; At request of the responsible minister.	Own initiative; A complaint; A referral by the canadian human rights Commission.	Can draft a special report at the request of parliament, or the responsible minister(s).	Own initiative; At the request of the responsible minister.
Reporting	Obligatory annual report to president of both houses of parliament and the responsible minister; Special reports first presented to the responsible minister, later to the Senate (upper house). Reports to parliament do not contain any classified information.	Obligatory annual report; Reports sent first to the executive who must place the report before parliament within 15 days; Issues special reports when requested by minister or on own initiative; Obligation to consult with the director of the intelligence service before making a report public.	Obligatory annual report to parliament the president, and responsible minister(s); Reports cannot contain information that could be harmful to national security.	Obligatory annual report; may also issue reports on any relevant matter; All reports are sent first to the prime minister who then submits them to parliament; The prime minister decides what information should be removed from the public version of the report.

	Belgium	Canada	South Africa	United Kingdom
Mandate	<p>Review the activities and methods of the intelligence services, their internal rules and directives;</p> <p>The committee should ensure: (1) the protection of constitutional and other rights by the intelligence services; (2) the coordination and effectiveness of the intelligence services;</p> <p>Investigate complaints;</p> <p>Provide advice on draft legislation, decrees and directives.</p>	<p>Review the services' performance of its duties and functions;</p> <p>Review directions issued by director of the intelligence service; service's regulations agreements with domestic and foreign entities; reports of the service and the IG;</p> <p>The committee should ensure that: (1) the service's activities comply with applicable law; and (2) the service does not exercise its powers in an unreasonable or unnecessary way;</p> <p>Direct the service or IG to conduct reviews of specific activities; or where it considers that this would be inappropriate, conduct such a review itself;</p> <p>Investigate complaints.</p>	<p>Review finances of intelligence services, including reports of the audit office;</p> <p>Receive complaints and order the IG or the intelligence services to investigate them;</p> <p>- Review reports of the IG;</p> <p>Make recommendations on intelligence-related legislation and any other matter related to national security and intelligence.</p>	<p>To examine the expenditure, administration and policy of the intelligence services.</p>
Investigative Powers	<p>Can summon any person to testify under oath before the committee;</p> <p>Can request the assistance of law enforcement authorities to force persons to comply.</p>	<p>When investigating complaints, the committee has the powers of a court: it may summon and enforce the appearance of persons before the committee, and can compel them to give oral or written evidence on oath.</p>	<p>May require any minister, a head of an intelligence service or the IG to appear before it;</p> <p>Right to hold hearings and subpoena witnesses.</p>	<p>May call on ministers and other relevant officials to testify.</p>

**Table 2: A comparison of selected intelligence oversight bodies in Belgium, Canada, South Africa and the United Kingdom<sup>12</sup>**

	<b>Belgium</b>	<b>Canada</b>	<b>South Africa</b>	<b>United Kingdom</b>
<b>Name</b>	Standing Intelligence Agencies Review Committee	Security Intelligence Review Committee	Joint Standing Committee on Intelligence	Intelligence and Security Committee
<b>Type</b>	Expert oversight body	Expert oversight body	Parliamentary oversight body	Parliamentary oversight body
<b>Other relevant oversight bodies</b>	Senate commission responsible for monitoring the Standing Intelligence Agencies Review Committee	Inspector General of the Canadian Security Intelligence Service (IG)	Inspector General for Intelligence (IG)	Intelligence Services Commissioner; Interception of Communications Commissioner; Investigatory Powers Tribunal
<b>Composition</b>	3 members; Must be at least one member from each linguistic group; Cannot hold elected office.	2-4 members; Cannot be members of parliament.	15 members of parliament	9 members of parliament drawn from both houses; Cannot be ministers (i.e. members of the executive).
<b>Appointment of Members</b>	Appointed by the Senate (upper house of parliament).	Appointed by the executive following consultation with the leaders of opposition parties.	Appointed by parliament through proportional representation, and on the basis of nominations by parties.	Appointed by the prime minister in consultation with the leader of the largest opposition party.
<b>Tenure of office</b>	5 years, renewable twice.	5 years, renewable.	Duration of parliament.	Duration of parliament.

## Parliament

### What is the role of parliament in overseeing intelligence services?

#### 1. Legislating

Parliaments draft and adopt the laws regulating intelligence services and establish institutions to oversee them. While drafting intelligence services legislation, members of parliament try to include comprehensive provisions on external oversight and accountability, respect for the rule of law and human rights. Parliaments also scrutinise, and if necessary, amend proposed legislation. Finally, parliaments identify and amend gaps in existing legislation.

#### 2. Controlling finances

Parliaments also control the intelligence services' use of public money; they approve future budgets and review past spending. Each year parliaments approve projected spending. During this process they are able to question the executive about their policies and priorities for the intelligence services. Parliament has the power to reject or limit funding if the executive and/or the intelligence services refuse to address its concerns. Thus, parliamentarians use their budgetary oversight role to influence the policies and actions of intelligence services.

In addition to approving prospective spending, parliaments are involved in reviewing past expenditures of intelligence services. In some states, parliaments have accounts committees that review all government expenditures. In other states, national audit institutions perform this function under the supervision of parliament.

#### 3. Overseeing policies and activities

Parliaments also oversee the administration, policies and operational activities of intelligence services. This helps to ensure they are fulfilling their mandate effectively and in accordance with the law. Parliamentary oversight of intelligence services is organised in a variety of ways. In

some states, parliamentary committees for defence or the interior may be responsible for intelligence oversight. However, an increasing number of states are establishing special parliamentary committees to oversee intelligence services (see pages 38-42). Elsewhere, parliament plays a more indirect role in overseeing the intelligence services. It mandates an external, expert body to carry out the day-to-day oversight of intelligence services. Parliament may play a role in appointing the members of expert oversight bodies. In many democratic states, such bodies report to parliament, which can then take action to ensure that the expert body's findings and recommendations are addressed.

Finally, parliaments oversee intelligence services by setting up inquiries into particular events or activities involving the intelligence services.

## Expert oversight bodies

### What is the role of expert intelligence oversight bodies?

An increasing number of states are establishing expert intelligence oversight bodies in addition to or instead of parliamentary oversight bodies. These bodies are independent from intelligence services, the executive and parliament. They focus exclusively on overseeing particular intelligence services. Expert oversight bodies are commonly mandated to oversee the legality of the work of intelligence services but their mandates may also include monitoring the effectiveness of operations, administrative practices, and the finances of intelligence services (see page 38 and Table 2).

Parliament usually appoints oversight bodies and they report to parliament and/or the executive. In contrast to members of parliamentary intelligence oversight committees, most members of expert oversight bodies are not members of parliament. They are normally senior public figures, including prominent members of civil society, current and former members of the judiciary and former politicians.

intelligence services, usually appoints directors of intelligence services. In many states, the executive must consult with leaders of opposition parties before appointing directors. They also may need to consult the parliament. Parliament may ask questions about the nominee, or in some cases, organise a hearing with him or her. The involvement of other stakeholders in the appointment of directors helps to prevent the executive from appointing persons who will protect or promote their own political interests.

### **Why are directors of intelligence services appointed for a fixed period?**

The law requires directors of intelligence services to be appointed for a fixed term of office. They can only be removed from office if they breach specific rules. A fixed term of office helps to protect directors' jobs from political pressures or changes in government. For example, fixed terms of office make it difficult for an executive member to force his or her own agenda on intelligence services by threatening to remove a director from office if he or she does not take a particular course of action.

## **The executive**

### **What role does the executive play in controlling and assessing intelligence services?**

In democratic societies, the executive has overall control of intelligence services. Members of the executive establish the overarching policies and priorities for intelligence services. Additionally, the executive is politically responsible for the intelligence services; it is accountable to parliament and the public for intelligence activities.

The executive is responsible for authorising intelligence activities that pose a significant risk to the safety of individuals, the state's foreign relations and/or its reputation. In authorising these activities the executive takes political responsibility and also provides additional controls over the intelligence services.

The executive oversees intelligence services to ensure they perform their functions effectively and in accordance with the law. If there are allegations of wrongdoing made against

intelligence services, the executive may initiate inquiries into particular intelligence activities.

While the activities of intelligence services are based on statutes, the executive issues regulations to help clarify and implement the laws. For example, the executive may issue guidelines on ethical standards based on statutes relating to intelligence services.

## **The judiciary**

### **What is the role of the judiciary in controlling and overseeing intelligence services?**

Judiciaries play an important role in controlling and overseeing intelligence services. In many states, they authorise and oversee the use of intelligence services' special powers (see pages 18-19 and Box 3). Courts also settle complaints made against the intelligence services and, if required, prescribe remedies for any wrongdoing (see pages 43-45). Through their rulings, courts set standards for controlling the future conduct of intelligence services.

Courts also adjudicate on matters concerning access to or disclosure of information relating to intelligence services. In many democratic states, individuals and civil society organisations are able to request information about any government agency. Gaining access to this information can enable society to oversee the activities of the government, including its intelligence services. Courts may be required to adjudicate on such claims concerning information about or held by intelligence services. These decisions are made on the basis of access to/freedom of information laws. Additionally, courts may be required to adjudicate on cases brought against persons accused of unlawfully disclosing classified information held by intelligence services.

Finally, in democratic states the executive may ask current or former judges to carry out judicial inquiries into past events or activities involving the intelligence services.

Third, their information gathering role has potential for disrupting political parties, media and other institutions and professions. The state needs to control intelligence services to protect such vital components of a democratic society.

Fourth, democratic societies need control over intelligence services because the law allows them to operate secretly. For example, they may secretly listen to an individual's communications or film and photograph their private homes. The individual may be unaware that intelligence services are taking measures against them. He or she is not in a position to challenge those actions. Furthermore, individuals and the public at large are unlikely to be able to monitor intelligence services' actions that are done in secret even when they are legal. Given that intelligence services are not subject to the same level of public scrutiny as other government agencies, the potential for ineffective or illegal practices is high. Hence, governments need control over secret operations to ensure intelligence services are performing their work effectively and in compliance with the law.

### Which institutions control and/or oversee intelligence services?

Five main types of institutions control and/or oversee intelligence services: the internal management of the intelligence service (pages 32-33), the executive (page 33), the judiciary (page 33), parliament (pages 34-42), and expert oversight bodies (pages 34-42).

## Internal management

### What role does internal management play in controlling intelligence services?

Internal management controls day-to-day intelligence activities. It ensures that intelligence officers conduct their work effectively and meet the executive's requirements. It is also responsible for the intelligence services' compliance with relevant national and international laws.

Internal management establishes procedures for assigning, reporting on and evaluating all intelligence activities. Additionally, it issues ethical codes of conduct and other guidance

for intelligence staff. Internal management also coordinates the processes for evaluating the performance of staff.

### To whom do intelligence services report?

Intelligence services report to the executive, parliament and the public. They report to the executive about their prospective, ongoing and completed activities. The executive uses intelligence services' reporting to evaluate whether they are fulfilling their mandate and meeting the overarching priorities for intelligence services.

Intelligence services report to parliament either directly or through the minister responsible for intelligence. Parliament uses intelligence services' reports to scrutinise intelligence activities and inform decision-making on future budget allocations for intelligence services. Intelligence services sometimes submit reports to the plenary of parliament which are usually public.

Intelligence services also report to independent intelligence oversight bodies; these reports often contain classified information. In some systems, intelligence services and/or the minister or ministers in charge report to a designated committee within parliament or an expert oversight committee that operates outside of parliament.

Intelligence services also write reports for public audiences. Public reports raise awareness of the work of intelligence services and foster public confidence. They are usually posted on the intelligence services' webpage.

National law generally requires intelligence services to report to parliament and/or the executive about their activities on a periodic basis such as every six months. Parliamentary and expert oversight bodies may request additional reports from intelligence services, or from the executive minister in charge of intelligence services, about particular issues.

### Who appoints directors of intelligence services?

National laws outline the procedures for appointing directors of intelligence services and the qualifications required by directors. The head of government, or the minister responsible for

be strictly necessary and proportionate to the threat. Additionally, intelligence services, like law enforcement agencies, must report all use of lethal force and will be subject to an investigation by an independent body.

### The control and oversight of intelligence services

#### Why do democratic societies control their intelligence services?

There are four main reasons why democratic societies control their intelligence services.

First, democratic societies hold elected leaders accountable for the work of all government agencies and bodies funded by public money. The intelligence services are no exception to this rule. Society must have control over intelligence services in order to account for public money used to employ staff and fund their activities.

Second, intelligence services have special powers for collecting information that are not available to other members of the society. These powers create the potential for violating human rights. Therefore, a democratic society controls intelligence services in order to protect the human rights of all individuals who come into contact with intelligence services.

#### Box 8: International standards on the use of force by public officials

The following extracts from the ICCPR, the UN Code of Conduct for Law Enforcement Officials, and the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials apply to intelligence services whenever they use force against a person<sup>11</sup>. If states give their intelligence services powers to arrest and detain, they should ensure that they conform to these standards, as well as all other applicable international and domestic law.

- Every human being has the inherent right to life. This right shall be protected by law. No one shall be arbitrarily deprived of his life (ICCPR, article 6.1)
- Law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty (CoC Law Enforcement Officials, principle 3)
- Law enforcement officials shall not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape, and only when less extreme means are insufficient to achieve these objectives. In any event, intentional lethal use of firearms may only be made when strictly unavoidable in order to protect life. (Principles on the Use of Force and Firearms, principle 9)
- Whenever the lawful use of force and firearms is unavoidable, law enforcement officials shall:
  - a. Exercise restraint in such use and act in proportion to the seriousness of the offence and the legitimate objective to be achieved;
  - b. Minimize damage and injury, and respect and preserve human life; (Principles on the Use of Force and Firearms, principle 11)
- Governments shall ensure that arbitrary or abusive use of force and firearms by law enforcement officials is punished as a criminal offence under their law. (Principles on the Use of Force and Firearms, principle 7)
- Governments and law enforcement agencies shall ensure that an effective review process is available and that independent administrative or prosecutorial authorities are in a position to exercise jurisdiction in appropriate circumstances. (Principles on the Use of Force and Firearms, principle 22)
- Persons affected by the use of force and firearms or their legal representatives shall have access to an independent process, including a judicial process. (Principles on the Use of Force and Firearms, principle 23)

### **Standards for the protection of persons in detention**

- All persons deprived of their liberty shall be treated with humanity and with respect for the inherent dignity of the human person. (ICCPR, article 10)
- No person under any form of detention or imprisonment shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. No circumstance whatever may be invoked as a justification for torture or other cruel, inhuman or degrading treatment or punishment. (UN Principles on Detention, principle 6; ICCPR article 7, CAT article 2.2-3)
- It shall be prohibited to take undue advantage of the situation of a detained or imprisoned person for the purpose of compelling him to confess, to incriminate himself otherwise or to testify against any other person. (UN Principles on Detention, principle 21.1)
- No detained person while being interrogated shall be subject to violence, threats or methods of interrogation which impair his capacity of decision or his judgement. (UN Principles on Detention, principle 21.2)
- States shall keep under systematic review interrogation rules, instructions, methods and practices as well as arrangements for the custody and treatment of persons subjected to any form of arrest, detention or imprisonment in any territory under its jurisdiction, with a view to preventing any cases of torture. (CAT, article 11)

### **Oversight and review of detention**

- Any form of detention or imprisonment and all measures affecting the human rights of a person under any form of detention or imprisonment shall be ordered by, or be subject to the effective control of, a judicial or other authority. (UN Principles on Detention, principle 4)
- Anyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings before a court, in order that that court may decide without delay on the lawfulness of his detention and order his release if the detention is not lawful. (ICCPR, article 9.4)
- Anyone who has been the victim of unlawful arrest or detention shall have an enforceable right to compensation. (ICCPR, article 9.5)
- States shall ensure that any individual who alleges he has been subjected to torture [...] has the right to complain to, and to have his case promptly and impartially examined by, its competent authorities. (CAT, articles 12-13)
- In order to supervise the strict observance of relevant laws and regulations, places of detention shall be visited regularly by qualified and experienced persons appointed by, and responsible to, a competent authority distinct from the authority directly in charge of the administration of the place of detention or imprisonment. (UN Principles on Detention, principle 29 .1)

Most democratic states do not permit their intelligence officers to use force of any kind. In fact, intelligence officers are subject to the same rules on the use of force as members of the public. Intelligence services must seek the assistance of the police if the use of force is required. Notably, intelligence services may call upon the police to arrest an individual who has committed or is about to commit a serious criminal offence. Additionally, intelligence officers may request that they are accompanied by the police on missions where their physical security may be threatened. For example, intelligence officers

may be accompanied by a police officer to execute a warrant to remove an object or install a listening device in a private house.

Some democratic states allow intelligence services to use powers of arrest and detention (see page 27). If, while performing an arrest, intelligence officers are faced with an imminent threat to their life or the life of others they may use lethal force. In such cases, they must comply with the same laws and regulations that apply to the use of force by law enforcement agencies (see Box 8). This means that any use of force must

**Box 7: International standards on arrest and detention**

International law regulates arrest and detention by all state institutions, including intelligence services. International human rights treaties, including the International Covenant on Civil and Political Rights (ICCPR) and the Convention Against Torture (CAT), contain a number of key provisions in this regard. The UN Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment (UN Principles on Detention) supplements the rules contained in these treaties.<sup>10</sup> While most democratic states do not permit their intelligence services to arrest or detain anyone, if intelligence services are given these powers they are required to comply with the following international standards.

**Legal basis for arrest and detention**

- Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law. (ICCPR, article 9.1)

**Procedural standards for arrest and detention**

- Arrest, detention or imprisonment shall only be carried out strictly in accordance with the provisions of the law and by competent officials or persons authorized for that purpose. (UN Principles on Detention, principle 2)
- Anyone who is arrested shall be informed, at the time of arrest, of the reasons for his arrest and shall be promptly informed of any charges against him. (ICCPR, article 9.2)
- There shall be duly recorded:
  - a. The reasons for the arrest;
  - b. The time of the arrest and the taking of the arrested person to a place of custody as well as that of his first appearance before a judicial or other authority;
  - c. The identity of the law enforcement officials concerned;
  - d. Precise information concerning the place of custody.
- Such records shall be communicated to the detained person, or his counsel, if any, in the form prescribed by law. (UN Principles on Detention, principle 12)
- The duration of any interrogation of a detained or imprisoned person and of the intervals between interrogations as well as the identity of the officials who conducted the interrogations and other persons present shall be recorded and certified in such form as may be prescribed by law. (UN Principles on Detention, principle 23.1)
- A detained person shall be entitled to have the assistance of a legal counsel. He shall be informed of his right by the competent authority promptly after arrest and shall be provided with reasonable facilities for exercising it. (UN Principles on Detention, principle 17.1)
- Promptly after arrest and after each transfer from one place of detention or imprisonment to another, a detained or imprisoned person shall be entitled to notify or to require the competent authority to notify members of his family or other appropriate persons of his choice of his arrest, detention or imprisonment or of the transfer and of the place where he is kept in custody. (UN Principles on Detention, principle 16.1)

mass destruction. It is most common for an intelligence service to have a mandate to use powers of arrest and detention in states that do not have a separate intelligence organisation, and to attach intelligence functions to the police. Under such systems, individuals who are responsible for intelligence collection are likely to do criminal investigations of terrorist acts and would be responsible for arresting and detaining individuals suspected of those crimes. In this context national law may need to authorise intelligence services to use powers of arrest and detention.

### What international standards apply to the use of powers of arrest and detention?

Democratic societies allowing intelligence officers to arrest and detain individuals incorporate into national law the internationally accepted standards related to arrest and detention (see Box 7).

These standards are applicable to intelligence services in the following categories:

the laws and rationale for arresting and detaining individuals; the treatment of individuals in detention; and the oversight and review of arrests and detention.

#### Laws

Intelligence services are prohibited by law from arresting and detaining people for the sole purpose of collecting information. The law, under special circumstances, may authorise them to arrest and detain individuals who have committed a crime against national security or present an imminent threat to national security.

#### Treatment of detainees

Intelligence services must respect the human rights of the individual who they have arrested and detained. There are actions they must take and actions they must refrain from taking. For example, intelligence services must ensure that a detained individual has access to a lawyer and is able to contact his or her family. Also, they must ensure a detainee has adequate living conditions while they are in detention. Intelligence services must refrain from any forms of mistreatment of detainees.

#### Oversight

Judicial oversight of detention is essential for preventing individuals from being detained arbitrarily. This oversight requires a court to review the legality of all detentions. The court, not the intelligence officer who arrested and detained individuals, determines whether there are legitimate grounds for ongoing detention. If detainees are not charged with a criminal offence they must be released. In addition, ombudsmen institutions or human rights monitoring bodies conduct inspections of detention facilities. In many states, such bodies may make unannounced visits to ensure that detainees are being treated correctly.

### Do intelligence services need their own detention facilities?

Democratic societies do not permit intelligence services to have their own detention facilities. In states that give the powers of arrest and detention to intelligence services, these organisations share the same detention facilities used by law enforcement agencies. Common detention facilities help to ensure that intelligence officers do not detain individuals arbitrarily and treat them in accordance with national laws which recognise internationally accepted standards on the treatment of persons in detention.

### The use of lethal force by intelligence services

#### Are intelligence services permitted to kill?

Intelligence services are not permitted to kill. International law prohibits states from killing any person except in three situations and then only under specific controls and restrictions: (1) In an armed conflict, a combatant may kill an enemy combatant, but only if a set of clearly defined conditions are met. (2) Law enforcement authorities may use lethal force if it is strictly necessary to prevent an imminent threat to life, and there is no other means for countering the threat. (3) Following judicial process, a court may impose the death penalty as a form of capital punishment for specific, serious criminal offences.

**Box 6: Croatian regulations on intelligence cooperation with foreign entities<sup>9</sup>**

The Act on the Security Intelligence System of the Republic of Croatia provides the legal basis for the Croatian intelligence services to cooperate with foreign entities, and outlines the controls that apply to sharing personal data with foreign entities.

**Article 59**

1. Based on their international commitments, the security intelligence agencies may cooperate with foreign security, intelligence and other corresponding services, through the exchange of information, equipment, through jointly conducted activities from their respective scopes, and through education of employees.
2. The establishment and the suspension of the cooperation with each foreign service are approved by the National Security Council on the basis of the recommendations of the directors of the security intelligence agencies and the previously obtained opinion of the Council for the Coordination of Security Intelligence Agencies.

**Article 60**

1. Security intelligence agencies may communicate to the appropriate foreign services the information on the citizens of the Republic of Croatia if they have been provided with relevant data indicating that such person is a threat to the national security of the state to which data is supplied, or to values protected by the international law. The information will not be provided if that would be contrary to the interests of the Republic of Croatia or if the protection of the interests of the person concerned is of greater value.
3. The delivered data must be entered into the records. Such data shall be accompanied by a notice indicating that they may only be used for the purpose they were provided for, and that the security intelligence agency providing the data retains its right to request feedback on how the provided information has been used.

Second, in some states intelligence services must inform an oversight body about transfers of information to foreign bodies. By knowing about transfers of information over time, an oversight body is able to monitor patterns and, if necessary, question particular cooperative relationships and activities of particular intelligence services. Oversight bodies may also examine the information intelligence services have sent to foreign bodies. Seeing the shared information enables them to question whether the decision to send information was necessary and appropriate in view of the possible implications for the human rights of the individuals concerned.

Third, external oversight bodies investigate allegations of wrongdoing linked to international intelligence cooperation. For example, they conduct inquiries into the actions of intelligence services in particular cases where individuals may have been mistreated.

## The intelligence services' use of powers of arrest and detention

### Should intelligence services have powers to arrest and detain individuals?

In most democratic societies national law does not allow intelligence services to use powers of arrest and detention. These powers usually support law enforcement rather than the intelligence services' information gathering role. International human rights law does not permit the arrest and/or detention of individuals for the purpose of collecting information.

However, some democratic states give intelligence services a mandate to arrest and detain individuals who have committed or are about to commit criminal offences threatening national security. For example, they may arrest persons involved in the preparation of terrorist attacks or the proliferation of weapons of

Finally, in addition to threats posed to human rights, international intelligence cooperation may damage a state's reputation and foreign relations. For example, intelligence services may cooperate with a foreign intelligence agency in ways that interfere with their state's foreign policy. Given this risk, states try to control their intelligence services' international cooperation as much as possible.

### How do states control international intelligence cooperation?

National laws regulate intelligence cooperation with foreign governments and intelligence services. Such laws and regulations specify who the intelligence services may cooperate with; what rationale and conditions must exist to cooperate with those bodies; and how the government will authorise and oversee such cooperation (see Box 6 on how international intelligence cooperation is regulated in Croatia).

In view of the risks associated with international intelligence cooperation, national laws require intelligence services to obtain approval from the executive before entering into an agreement with a foreign body. In addition, the executive must usually approve joint operations or activities involving the sharing and exchange of information posing risks. Executive approval of international intelligence cooperation, especially sensitive activities, ensures that intelligence services do not operate unchecked by the state.

### What controls apply to the sharing of information with foreign intelligence services?

Democratic societies have laws and regulations to control intelligence services' information sharing with foreign intelligence services (see Box 6). Laws restrict when and under what circumstances intelligence services may share information with foreign bodies. For example, intelligence services will only ask for information from foreign bodies if the information is necessary to fulfil their mandate. Likewise, they will not give information to foreign bodies unless the information is necessary for them to fulfil their mandate.

In addition, the law requires intelligence services to consider whether or not sharing of specific information will be in the best interests of the

state. For example, some laws require intelligence services to consider whether sharing information with a foreign entity would serve the state's foreign policy. More importantly, intelligence services are required to consider the effects sharing of information may have on the individuals who are the subjects of the information. In democratic societies laws prohibit sharing information with foreign bodies if the information is likely to endanger the lives of individuals or lead to other human rights violations.

In addition to the laws and regulations governing intelligence work, intelligence services have their own conditions for sharing information with foreign partners. The most common examples are the principles of "originator control" and "third party rule". These informal rules apply to most international intelligence sharing. "Originator control" refers to the principle that the intelligence body giving the information dictates the limits to the use of the information. "Third party rule" means the recipient of the information is not allowed to share the information with another agency or other third party without the permission of the intelligence services that originally provided the information. These principles help to prevent unauthorised disclosure of sensitive information.

Intelligence services also attach notes to shared information that are often referred to as "caveats". These notes outline how the shared information may be used. For example, they may prohibit a foreign agency from using particular information as the basis to arrest and detain someone. Intelligence services retain the right to ask the foreign body to whom they have given information how the information has been used. Such informal rules help to minimise the misuse of information by foreign bodies and may promote more respect for human rights.

### How is international intelligence cooperation overseen?

In democratic societies, external oversight bodies monitor international intelligence cooperation to ensure that it complies with the law. They monitor intelligence cooperation in several ways. First, they examine intelligence services' agreements with foreign partners to ensure agreements comply with the law.

In some cases laws and regulations permit intelligence services to refuse requests from individuals to access their personal data. For example, they may deny requests in order to keep an ongoing investigation out of the public domain, to ensure public safety or to protect national security interests. Intelligence services do not usually have to give individuals reasons for denying their requests. However, external oversight bodies may scrutinise intelligence services' decisions to deny requests. Individuals may be able to appeal to such bodies to review their case. This helps to ensure that decisions to deny access to personal data are strictly necessary.

### International intelligence cooperation

#### What is international intelligence cooperation?

The term "international intelligence cooperation" describes the ways in which intelligence and security services of two or more countries work together. Intelligence services cooperate with foreign entities in three main ways. First, and most commonly, intelligence services share information with their foreign counterparts. They may share and/or exchange raw data or provide analyses of information to foreign intelligence services.

Second, some intelligence services conduct joint operations with their foreign partners. For example, agents from different intelligence services may collaborate to collect information. Or intelligence services of one country may share their intelligence infrastructure with foreign intelligence services.

Third, international intelligence cooperation may involve the sharing of knowledge and expertise. For example, intelligence services may train foreign counterparts or send intelligence officers to support the work of foreign intelligence services.

#### Why do intelligence services cooperate with foreign governments and intelligence services?

Intelligence services cooperate with foreign partners mainly because this collaboration gives them greater access to information and expertise. Intelligence services in one country may not

have enough resources or expertise to collect information about relevant threats existing in all regions of the world. Thus, they need to rely on foreign agencies; these partners have the geographical position and knowledge of specific groups, languages and cultures to collect the needed information. Intelligence services in one country may provide information to a foreign counterpart agency in exchange for information or other resources, such as equipment or money. International cooperation between intelligence services has become increasingly important because groups threatening the security of states and their populations often operate across borders and in a number of states.

#### What are the risks of intelligence cooperation?

Cooperation among foreign governments and intelligence services presents a variety of risks for all concerned parties. First, international cooperation poses significant risks to human rights protected under international law. Intelligence cooperation poses a particular threat to human rights when intelligence services share personal data with foreign entities. For example, an intelligence service that has received the personal data may end up using it in a way that violates human rights. They may use the personal data to identify individuals and detain them unlawfully and/or mistreat them. Generally, intelligence services tell a foreign partner how the personal data they share can be used, but ultimately they have little control over its use.

Second, in many cases intelligence services do not know how foreign bodies collect information or whether information was obtained legally. Specifically, they may not know whether a foreign body used torture or other unlawful tactics to obtain the information. However, if intelligence officials know that information obtained from foreign or domestic sources involved violating human rights, they can be considered complicit.

Third, some intelligence services may wish to cooperate with foreign partners in order to prevent their authorities from controlling their activities. Specifically they may want to avoid the legal controls and oversight their authorities may use to hold them accountable for respecting human rights while using their special powers for collecting information.

processing personal data in accordance with laws and regulations. They may check files on their own initiative or respond to individuals' enquiries about their files. In some states, the law requires intelligence services at times to inform oversight bodies when they share personal data with other institutions or when they delete information from their data files. Finally, in many states, oversight bodies scrutinise intelligence services' handling of requests made by individuals to access their personal data held by intelligence services (see Box 5).

### Can individuals access their personal data?

In democratic states, members of the public have the right to apply to access their personal data held by intelligence services. (See Box 5 for an example of how this process works in Germany). To gain access to their personal data they submit a request directly to the intelligence services or through the member of the executive responsible for intelligence services. After viewing their personal data, they may be able to submit requests to delete and/or change data.

#### Box 5: German law on access to personal data held by intelligence services<sup>8</sup>

German law gives people a general right to access their personal data held by the intelligence services. Applications are submitted directly to the intelligence services. The following extracts illustrate how this process works.

##### Applying to access personal data held by the intelligence services

- The Federal Office for the Protection of the Constitution shall provide the data subject, at his/her request, with information free of charge on personal data stored on him/her, if he/she refers to concrete matters and proves to have a special interest in the information which he/she has asked for.

##### Grounds for refusing access to personal data

- The information shall not be provided if:
  1. this would prejudice the proper fulfillment of tasks,
  2. this could expose sources, or if it is to be feared that the Federal Office for the Protection of the Constitution's knowledge or its modus operandi might be explored,
  3. this would impair public safety or otherwise be detrimental to the Federation or a Federal State, or if
  4. the data or the fact that they are being stored must be kept secret in accordance with a legal provision or by virtue of their nature, in particular on account of an overriding justified interest of a third party.
- The decision shall be made by the head of the Federal Office for the Protection of the Constitution or by a staff member explicitly authorised by him.
- The obligation to provide information shall not include information on the origin of the data and the recipients of the data transferred.
- Reasons for the refusal to provide information need not be given if this jeopardised the purpose being pursued by refusing to provide the information. The reasons for the refusal shall be taken on record.

##### Right to appeal

- In case of a refusal to provide information the data subject shall be informed of the legal basis for a reason not being given and of the fact that he/she may appeal to the Federal Commissioner for Data Protection, who shall, at his request, be supplied with the information unless the Federal Ministry of the Interior determines in a particular case that this would jeopardise the security of the Federation or a Federal State.

### Who oversees the use of personal data and what do they do?

External oversight bodies oversee intelligence services' use of personal data to ensure they use data in accordance with the law. Such bodies include parliamentary and expert oversight bodies, as well as data protection institutions (see pages 34-42).

These oversight bodies scrutinise intelligence services' decisions to retain personal data and create files on certain individuals. In some states an oversight body must give intelligence services its consent before creating a file on an individual.

Oversight bodies also check the files of intelligence services to make sure they are

#### Box 4: Regulations on the use of personal data by the German Federal Office for the Protection of the Constitution <sup>7</sup>

German law imposes strict controls on the use of personal data by the Federal Office for the Protection of the Constitution (Germany's domestic intelligence service). The following extracts from two German laws are examples of good practice on the collection, retention and deletion of personal data. In Germany, all of these activities are monitored by the G10 Commission, an independent oversight body which has access to all information held by the intelligence services.

#### Permissible grounds for using personal data

- To fulfill its tasks, the Federal Office for the Protection of the Constitution may store, modify and use personal data if:
  1. there are actual indications of efforts or activities pursuant to section 3, subsection 1 (these activities include: efforts directed against the free democratic basic order, the existence or the security of the Federation or one of its States, or aimed at unlawfully hampering constitutional bodies of the Federation or one of its States in the performance of their duties)
  2. this is necessary for the investigation and analysis of efforts or activities pursuant to section 3, subsection 1 or
  3. the Federal Office for the Protection of the Constitution takes action under section 3, subsection 2. (that is, against activities threatening security or intelligence activities carried out on behalf of a foreign power)

#### Regulations on the storage, correction and erasure of personal data held by the Federal Office for the Protection of the Constitution

- The Federal Office for the Protection of the Constitution shall restrict the duration of storage (of personal data) to the extent necessary to fulfill its tasks.
- Incorrect personal data stored in files shall be corrected by the Federal Office for the Protection of the Constitution.
- When dealing with particular cases, the Federal Office for the Protection of the Constitution shall check within given periods, after five years at the latest, if stored personal data must be corrected or erased.
- Personal data stored in files shall be erased by the Federal Office for the Protection of the Constitution if their storage was inadmissible or knowledge of them is no longer required for the fulfillment of its tasks. The data shall not be erased if there is reason to believe that erasure would impair legitimate interests of the data subject. In this case the data shall be blocked and shall only be transferred with the data subject's consent.

#### Oversight

- The (G10) Commission's supervisory powers shall extend to the entire scope of collection, processing and use of the personal data obtained pursuant to this Act by intelligence services of the Federation.

In exceptional circumstances, intelligence services are also allowed to share personal data with foreign governments and their agencies. For more information please refer to the International Intelligence Cooperation section of this guidebook.

### Why do democratic societies restrict the use of personal data?

Democratic societies restrict the use of personal data by intelligence services for three main reasons. First, democratic societies restrict the use of personal data because of the inherent risks the disclosure of personal data may pose to individuals. Personal data includes information about the most private aspects of a person's life, including their medical records, religious beliefs, political opinions and personal relationships. Disclosure of such information may jeopardise their employment prospects, personal and professional relationships and personal safety.

Second, there is the potential risk that intelligence services and/or others who may have legal access to an individual's personal data will use it for illegal purposes. For example, intelligence services and/or the executive may be tempted to use personal data to discredit or blackmail political opponents. Therefore democratic governments need to restrict uses of personal data through legislation.

Finally, individuals do not normally know what personal data an intelligence services holds about them. Consequently, they may not be able to challenge the intelligence services' use of their personal data or the accuracy of the data. Therefore, it is essential that laws set clear rules for using personal data, and that oversight bodies monitor compliance with these rules.

### What legal controls apply to the use of personal data?

Intelligence services need to collect and make use of certain personal data in order to perform their functions. In particular, they need to be able to identify particular individuals and collect information on their behaviour and activities in order to identify possible threats to national security. With this in mind, states adopt laws permitting intelligence services to use certain personal data without the consent of the individuals concerned. Through legislation

they also apply strict controls to regulate the use of personal data. (See Box 4 for an example of legislation on the use of personal data by intelligence services in Germany). These controls are complex; the following discusses just three types of legal controls.

First, national laws control what types of personal data intelligence services may use. For example, laws permit intelligence services to use personal data of individuals involved in activities which threaten national security, such as their membership of a terrorist organisation. Laws require that the use of personal data is linked to a person's behaviour; that is, their involvement in activities that threaten national security. Democratic societies prohibit intelligence services from using personal data on the basis of characteristics such as a person's ethnicity, religion, or gender. In addition, laws prohibit intelligence services from using parts of an individual's data that are not linked to a national security threat, such as their medical records, even if they are involved in activities that threaten national security.

Second, laws place limits on retaining personal data. Intelligence services can only retain personal data if it is necessary for identifying and analysing a specific threat to national security. Laws require intelligence services to check their files regularly in order to update personal data files. In many democratic societies national law requires intelligence services to delete personal data that is no longer relevant or necessary, such as personal data of individuals who pose no threat to national security.

Third, the law controls access to personal data held by intelligence services. Only certain employees of intelligence services may access personal data files. The law also requires them to document all access of personal data files by these individuals. These controls aim to prevent the misuse of personal data.

Fourth, the law restricts intelligence services' release of personal data for use by other government agencies. They may only share personal data with authorised government bodies which need the information to carry out their mandates. Strict limitations are placed on the way such bodies can use personal data shared with them by intelligence services.

- a. to enter any place or open or obtain access to any thing;
- b. to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or
- c. to install, maintain or remove any thing.

#### **Matters to be specified in warrant**

4. There shall be specified in a warrant issued under subsection (3)
  - a. the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(a) to (c) authorized to be exercised for that purpose;
  - b. the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;
  - c. the persons or classes of persons to whom the warrant is directed;
  - d. a general description of the place where the warrant may be executed, if a general description of that place can be given;
  - e. the period for which the warrant is in force; and
  - f. such terms and conditions as the judge considers advisable in the public interest.

## **Use and management of personal data**

### **What is personal data?**

Personal data is information about a given individual. This includes facts such as a person's contact details, date of birth, and passport and social security numbers. Personal data also includes more detailed information about a person's private life, such as their health and employment records, religious beliefs or political opinions, details of memberships of political parties and trade unions, and details about their relationships with partners and friends. Intelligence services may need to collect personal data on individuals to identify possible threats to national security.

### **How do intelligence services acquire personal data?**

Intelligence services acquire personal data in five main ways. First, intelligence services collect personal data from public or open sources. Second, they acquire personal data through the use of special powers, such as secretly monitoring communications (see page 17). Third, they may request information and personal

data about a specific individual from domestic governmental agencies such as immigration services. Fourth, informants may provide personal data to intelligence services. Finally, intelligence services may acquire personal data about specific individuals from foreign governments and/or their intelligence services.

### **How do intelligence services and their governments use personal data?**

Intelligence services retain much of the personal data they collect in electronic or paper files for easy access. First, they use these files to support ongoing and future investigations of threats to national security. They may also use personal data to assess individuals applying for government security clearance.

Second, intelligence services share personal data with government agencies and officials such as law enforcement authorities and prosecutors. Governments are increasingly using personal data from intelligence services to support taking legal actions against specific individuals. They use personal data in counter-terrorism operations to justify banning travel, denying visas, seizing assets and restricting an individual's movements and communications with others.

**Box 3: The process for authorising the use of special powers by the Canadian Security Intelligence Service<sup>6</sup>**

The Canadian Security Intelligence Service Act outlines the steps for the application and issuing of warrants for the intelligence services to use special powers. Any application to use special powers must be approved by both the executive and a judge.

**Application for warrant**

Section 21.

1. Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.

**Matters to be specified in application for warrant**

2. An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,
  - a. the facts relied on to justify the belief, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16;
  - b. that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (a) would not be obtained;
  - c. the type of communication proposed to be intercepted, the type of information, records, documents or things proposed to be obtained and the powers referred to in paragraphs (3)(a) to (c) proposed to be exercised for that purpose;
  - d. the identity of the person, if known, whose communication is proposed to be intercepted or who has possession of the information, record, document or thing proposed to be obtained;
  - e. the persons or classes of persons to whom the warrant is proposed to be directed;
  - f. a general description of the place where the warrant is proposed to be executed, if a general description of that place can be given;
  - g. the period, not exceeding sixty days or one year, as the case may be, for which the warrant is requested to be in force that is applicable by virtue of subsection (5); and
  - h. any previous application made in relation to a person identified in the affidavit pursuant to paragraph (d), the date on which the application was made, the name of the judge to whom each application was made and the decision of the judge thereon.

**Issuance of warrant**

3. Notwithstanding any other law but subject to the Statistics Act, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2) (a) and (b) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

special powers they require the authorisation of a designated external body (see Box 3 for details of this process in Canada). Intelligence services submit a request to the designated body, justifying their need to use a specific special power. The authorising body will then make sure their specific request complies with the law.

Usually, a member of the executive, such as the minister responsible for intelligence services, or a court is responsible for authorising the use of special powers. However, the court is likely to be designated as the oversight body for cases involving significant intrusions into the lives of individuals, such as search and seizure of property and the monitoring of communications. Courts are fully independent from both the intelligence services and the executive and are in a good position to objectively analyse the requests to use special powers.

Some states require both the executive and the judiciary to authorise intelligence services' use of special powers (see for example, the Canadian model outlined in Box 3). This approach provides an additional check for ensuring that uses of special power are legal, necessary and worth pursuing given the risks involved.

### How does the state authorise the use of special powers?

The process for authorising the use of special powers differs between states and often depends on the specific power intelligence services want to use. However, laws normally require that the following three steps are taken before intelligence services can use special powers (see Box 3).

First, a designated member of the intelligence services writes a request to use a specific power which normally includes:

- a description of the activity and the specific individuals and/or groups the intelligence services want to investigate;
- an explanation of the efforts intelligence services have already made to collect information and what those efforts achieved;
- the special method they want to use and exactly what they will do such as monitor calls on a specific phone line; and

- a justification addressing why the use of the special power is necessary and beneficial for the investigation.

Second, the authorising body examines the request and assesses whether:

- the proposed use of special powers complies with all relevant laws;
- the use is necessary and beneficial; and
- the use is proportionate to the level of threat posed by the activity under investigation.

Third, the authorising body issues a warrant outlining the specific measures it authorises and how long those measures may be used.

The request and authorisation process described above is documented so intelligence services and oversight bodies may later evaluate the decisions taken.

### How do democratic societies oversee the use of special powers?

In democratic societies the executive and/or a designated oversight body oversee intelligence services' use of special powers by monitoring ongoing operations and reviewing completed operations.

Intelligence services provide regular reporting to the executive and/or designated oversight body on their progress during the operation. They provide summaries of information collected, progress made, and problems they have encountered. This reporting allows overseers to assess whether the use of special powers is both legal and necessary for the intelligence services to fulfil their mandate. The executive and/or a designated oversight body may terminate the use of a special power if intelligence services have failed to comply with one or all legal controls on the use of a special power, or if an oversight body determines it is no longer needed.

Finally, oversight bodies conduct reviews of the use of special powers once they are completed. In some states, oversight bodies can order intelligence services to delete information collected in illegal ways. External oversight bodies also review uses of special powers to identify trends that may help the government and the intelligence services address specific problems.

### What information are intelligence services not permitted to collect?

Intelligence laws restrict what types of information intelligence officers are permitted to collect. First, laws prohibit them from collecting information about individuals and activities posing no threat to national security

Second, in a democratic society laws usually prohibit intelligence officers from collecting information about lawful political and social activities. For example, they are not permitted to collect information about the lawful activities of political parties and their members, or about groups involved in peaceful protests. These legal prohibitions protect human rights and other values democratic societies consider important, such as the freedoms of association and assembly.

Finally, laws usually prohibit intelligence officers from collecting information for promoting particular interests. For example, the law does not permit them to spy on the political opponents of a particular party.

### Why do states restrict the collection of information from certain professions?

Members of some professions such as journalists, parliamentarians, lawyers, clergy and medical doctors have information which may be of interest to the intelligence services. However, many democratic societies have adopted laws and measures to restrict or prevent intelligence services from collecting information from or about individuals from these professions. For example, the law may prohibit collecting information about these individuals unless the intelligence services can prove that they are directly involved in activities posing a grave threat to national security. Additionally, democratic societies apply special controls for collecting information about members of certain professions. Notably, some states require their intelligence services to get the consent of the speaker of parliament before investigating parliamentarians.

Democratic societies restrict the collection of information from certain professions in order to protect the services they provide to the population. For example, lawyers help detainees to exercise their rights to liberty and a fair trial.

If intelligence services monitor communications passed between lawyers and detainees they will violate a detainee's right to confidential access to a lawyer. Journalists provide another example. They investigate issues of interest to the public and rely on confidential communications to develop their stories. This role is essential for overseeing the activities of government agencies and uncovering wrongdoing. If intelligence services monitor journalists' communications they may jeopardise the valuable work of the media.

### How does a democratic society control the use of special powers?

States legislate to give intelligence services special powers to collect information about threats to national security. Special powers are measures that are not lawfully available to other government agencies (with the exception of some police bodies) or members of the population (see page 17).

Democratic societies define and restrict intelligence services' use of special powers through legislation and regulations that outline:

- Who they are and are not permitted to investigate;
- What information they are and are not permitted to collect;
- What measures they are permitted to use to collect information;
- When they are and are not permitted to use these special powers; and
- How long they are permitted to use them for.

Democratic societies control intelligence services' use of special powers through organisations and processes created for authorising, overseeing and evaluating uses of special powers.

### Who authorises the use of special powers?

In democratic societies the use of special powers is the exception rather than the rule. Democratic societies impose strict controls on the use of such powers in order to minimise the risks that accompany their use. For this reason, each time intelligence services want to use their

### 3. Derogating from human rights obligations during a state of emergency

International human rights law permits states to temporarily derogate from some of their human rights obligations during a state of emergency. A state may proclaim a state of emergency in exceptional circumstances where the “life of the nation” is threatened. This includes serious and imminent threats to the physical security of the population and/or the functioning of democratic institutions.<sup>5</sup> The decision to declare a state of emergency and to derogate from specific rights is taken by the executive. Intelligence services are not involved in this process.

Upon announcing a state of emergency, a state must notify the relevant treaty body and specify which human rights will be suspended or limited. Suspensions or limitations of specific rights must be temporary, strictly necessary for dealing with the emergency, and proportionate to the threat faced. In addition, any suspensions or limitations of rights must be subject to the review of the judiciary and parliament. States are not permitted to derogate from any of the non-derogable rights mentioned above, or any other non-derogable rights listed in regional and international human rights treaties. Accordingly, national constitutional provisions on emergency powers cannot be used to justify actions that violate international human rights law.

If intelligence services are given additional powers to restrict human rights during a state of emergency, they must continue to comply with both international and domestic human rights law. Their activities must remain under the control and oversight of the executive, parliament, the judiciary, and any expert oversight bodies that exist.

## Information collection

### How do intelligence services collect information?

In democratic societies intelligence services collect much of the information they need to fulfil their mandate from public sources such as media articles, reports provided by governmental and non-governmental organisations and academic publications. Intelligence services also collect information from persons who have (or could gain) access to relevant information. For example,

members of groups that threaten national security may act as informers by secretly passing information to intelligence services. Intelligence services may also use persons with aliases or false identities to infiltrate organisations and provide information about their activities.

Individuals and groups who are planning to threaten national security do not usually disclose their intentions. Consequently, democratic societies need legislation enabling the intelligence services to gather information that cannot be found in the public domain. Thus, legislation gives the intelligence services special powers that are not usually available to other members of society. These special powers fall into four main areas.

First, legislation may permit intelligence services to monitor an individual’s verbal, electronic and paper-based communications without their consent. Such activities can require highly developed and complex technical means.

Second, legislation may also allow intelligence services to secretly film and photograph individuals and their property without their consent.

Third, legislation may permit intelligence services to give false identities to its agents to allow them to infiltrate groups which threaten national security.

Finally, legislation may allow them to make official requests to other government agencies or private companies for information about people even when it may infringe on their right to privacy. For example, they may sometimes be allowed to request an individual’s phone records from a telecommunications provider.

### What information are intelligence services permitted to collect?

In democratic societies, national laws control the information that intelligence services are permitted to collect. Laws permit intelligence services to collect information about specific activities posing a threat to national security, as defined in their legal mandate. They are only permitted to collect information about individuals and groups engaged in such activities if the information is relevant and necessary for carrying out their mandate.

include the right to life, freedom from torture and other inhuman or degrading treatment, the right to fair trial, the right to recognition before the law, freedom from slavery and involuntary servitude, and the prohibition on abduction and unacknowledged detention.<sup>3</sup> International humanitarian law supplements and reinforces these prohibitions in times of armed conflict; common article 3 of the Geneva Conventions outlines these minimum standards (see Box 2). Intelligence services are not permitted to take any action that infringes upon these rights at any time.

### Box 2: Extract from Common Article 3 of the Geneva Conventions<sup>4</sup>

In the case of armed conflict not of an international character occurring [...] each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

1. Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed “hors de combat” by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:
  - a. violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
  - b. taking of hostages;
  - c. outrages upon personal dignity, in particular humiliating and degrading treatment;
  - d. the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.

## 2. Human rights that may be limited

International human rights law permits states to limit certain human rights and freedoms of given persons. These include the rights to liberty, and privacy, and the freedoms of movement, association and expression. States can only take measures that limit the exercise of rights if such measures comply with the following criteria:

1. based on law that is public;
2. pursue a legitimate purpose (such as to protect national security, public safety or the human rights and freedoms of others);
3. be necessary in a democratic society;
4. proportionate to stated aims;
5. consistent with other human rights obligations. States violate the human right in question if they fail to comply with these requirements.

In many states, the law authorises intelligence services to limit the right to privacy by giving them special powers to collect information from/about individuals or groups suspected of involvement in specific activities that threaten national security, public safety and human rights (see pages 17-18). These special powers include measures like monitoring a person’s communications without their knowledge or secretly filming their activities. Such measures clearly limit a person’s right to privacy. Some states also mandate their intelligence services to perform law enforcement functions (see page 28). In this context, national law gives them the power to arrest and detain persons who are suspected of having committed specific crimes. These powers limit the rights to liberty and freedom of movement.

Democratic states impose strict controls on their intelligence services’ use of these powers in order to make sure they comply with international standards. They ensure that such powers are regulated by law, authorised and overseen by institutions outside the intelligence services (see pages 19-21).

### How do democratic societies ensure intelligence services uphold the law?

Intelligence services, like all other government agencies, are required to respect both international and national law. Of particular importance, are provisions of international human rights law and international humanitarian law. A state's national law on intelligence services must be compatible with its international legal obligations.

All intelligence services and their staff are required to comply with the law. The executive must also act in accordance with the law. The political authorities are not permitted to issue orders to the intelligence services that would require them to take illegal action.

Members of the executive are legally responsible for directives issued to intelligence services. Employees of intelligence services are individually responsible for ensuring that their own actions comply with the law. In many states, the law not only requires them to make sure that their actions comply with the law but also obliges them to disobey orders which would violate national or international law. Thus, a member of an intelligence service would have to answer for his or her unlawful behaviour and could face legal prosecution, even if it had been ordered by a superior. Given the extensive powers that can be given to members of intelligence services, such individual responsibility is particularly important as a safeguard against serious crimes, including human rights violations such as torture and extrajudicial killings.

It is therefore, critically important that the judiciary holds intelligence officers and, if required, members of the executive accountable under the law. Their individual decisions and actions can be challenged in a court; the rulings of a court are binding on the executive, as well as the intelligence services and their staff.

### What are the international legal standards guiding intelligence services?

As an institution of the state, intelligence services must comply with the government's international legal obligations. The state's obligations under international human rights law, in particular the civil and political rights outlined in the UN

Charter and the International Covenant on Civil and Political Rights, apply to intelligence services. These include the rights to life, liberty, fair trial, privacy and freedom of expression and association.

International standards on law enforcement activities are also relevant to intelligence services if national law permits them to perform law enforcement tasks such as arrest and detention.

In 2009 and 2010 the UN reviewed existing international legal standards and institutional controls applying to intelligence services. The UN Human Rights Council mandated a study of good practices on the legal and institutional frameworks for intelligence services and their oversight. This study compiled 35 noteworthy international practices and was presented to the Human Rights Council in June 2010 (see list of references).

### Are intelligence services permitted to violate human rights?

International human rights law does not permit states (including their intelligence services) to violate the human rights of anyone under their jurisdiction. In common with all government agencies, intelligence services must comply with international human rights law. In situations of armed conflict, intelligence services must also comply with international humanitarian law. States ensure that these international legal standards are implemented in their domestic law.

International human rights law establishes three categories of human rights and freedoms:

- (1) Rights that can never be limited or derogated from in any circumstances;
- (2) Rights that can be limited for specific reasons and in accordance with strict legal criteria;
- (3) Rights that can be suspended or limited during an armed conflict or state of emergency which threatens the existence of the state.

#### 1. Human rights that can never be limited or derogated from

International human rights law prohibits states and their agencies from limiting or derogating from certain human rights in any situation. These

Third, a legal basis gives intelligence services legitimacy in the eyes of the public. A publicly available law promotes an understanding of what the roles of the intelligence services are, and why they require public money to perform these tasks. This can help to ensure public support for the intelligence services.

Finally, public intelligence laws are needed to hold the government accountable. Intelligence oversight bodies and the public at large hold the executive and intelligence services to account for their compliance with such laws. Public laws also enable individuals to seek justice if they believe intelligence services have committed illegal actions against them.

### Are intelligence laws secret?

In democratic states, the fundamental laws governing intelligence services are in the public domain. As discussed on page 13, the public needs to know what the roles of the intelligence services are, and what powers they have for performing these tasks. Members of the public also need to know when and under what conditions the intelligence services would be allowed to restrict individual rights for national security purposes. Therefore, intelligence services' authority to restrict human rights must be contained in public laws.

The government may however, issue “subsidiary regulations” – such as “decrees” and “ministerial instructions” – that are not made available to the public. The law authorises the government to issue such regulations when it believes that making specific information available to the public could jeopardise the work of intelligence services and/or national security more generally. Regulations that are not made public typically contain information related to the operational methods of intelligence services, such as their use of particular devices or technologies. Such information is often not made public because it could give persons knowledge that could enable them to avoid detection by intelligence services, or to uncover persons working for services. This may undermine the effectiveness of intelligence services, pose a threat to the safety of people working for them, and may ultimately harm national security.

Regulations that are not made public must still comply with existing public laws and the

constitution. For example, they cannot authorise intelligence services to take actions violating human rights under international law.

### What do intelligence laws cover?

Intelligence laws allow states to regulate and oversee intelligence services. These laws cover the following areas. First, intelligence laws outline the mandate of intelligence services and provide a comprehensive list of their tasks. The mandate normally contains definitions of what constitutes a threat to national security. These laws limit the role of intelligence services in order to prevent intelligence officers from promoting interests other than those of the state and its population.

Second, intelligence laws provide a comprehensive list of the powers available to the intelligence services, and regulate how such powers can be used. Laws only permit intelligence services to use these powers in the context of their mandate. They limit the use of powers that may result in restricting individual rights for national security purposes.

Third, intelligence laws describe the structure and composition of intelligence services including the organisational responsibilities of divisions within the services.

Fourth, intelligence laws outline how governmental and non-governmental entities oversee intelligence services. For example, they regulate the process for appointing senior intelligence managers, and outline the mandates and powers of parliamentary and expert oversight bodies.

Fifth, intelligence laws describe the professional relationships intelligence services have with other governmental and non-governmental organisations and international organisations. For example, laws describe the processes the intelligence services use to exchange information or conduct joint operations with other organisations.

Sixth, intelligence laws often provide regulations guiding the use of personal data by intelligence services (see pages 21-25).

Finally, intelligence laws describe the processes individuals use if they want to make complaints about intelligence services' actions taken against them (see pages 43-46).

## Legal framework for intelligence services

### How do democratic societies provide a legal basis for intelligence services?

Some democratic states include general provisions on intelligence services in their constitutions. These constitutional rules are normally general provisions, such as the requirements that intelligence services are accountable to parliament and respect the rule of law (see Box 1 for the South African constitutional provisions on intelligence and security services).

Most democratic states have specific legislation on intelligence services, which forms the primary legal basis for regulating intelligence activities. Laws on privacy, data protection, the security of information, and access to information also provide important regulations for intelligence services. On top of this, the executive issues so called “executive orders”, “directives” and other regulations which supplement legislation. Such regulations are always based on existing legislation, and therefore need to comply with it.

### Why do intelligence services need a legal basis?

Democratic societies make sure that intelligence services operate in accordance with national laws. A legal basis for intelligence services is important for four main reasons.

First, the law clearly defines the mandate, role and responsibilities of intelligence services and their officials. Laws also define the activities they are permitted to perform. Governments depend on the law in order to control intelligence services.

Second, a legal basis for all government organisations is essential for promoting transparency. Public laws make society aware of the functions and powers of the government. Intelligence services have a legal basis for carrying out special powers to collect information that is not generally available to other government agencies or private individuals. For example, laws may permit them to use particular measures for investigating individuals. Individuals need to know how intelligence services can affect their personal lives and whether intelligence officers are respecting individual rights under the law.

#### Box 1: South African constitutional provisions on the intelligence and security services<sup>2</sup>

The Constitution of the Republic of South Africa includes a number of general provisions on the intelligence and security services.

- National security must be pursued in compliance with the law, including international law.
- National security is subject to the authority of Parliament and the national executive.
- The security services must be structured and regulated by national legislation.
- The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic.
- Neither the security services, nor any of their members, may, in the performance of their functions
  - a. prejudice a political party interest that is legitimate in terms of the Constitution; or
  - b. further, in a partisan manner, any interest of a political party.
- To give effect to the principles of transparency and accountability, multi-party parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.
- National legislation must regulate the objects, powers and functions of the intelligence services.

Table 1: Examples of the mandates and functions of intelligence services<sup>1</sup>

Country	Mandates and functions of the civilian intelligence services
<b>Canada</b>	<ul style="list-style-type: none"> <li>• The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.</li> <li>• The Service may provide security assessments to departments of the Government of Canada.</li> <li>• The Service may:               <ul style="list-style-type: none"> <li>a. advise any minister of the Crown on matters relating to the security of Canada, or</li> <li>b. provide any minister of the Crown with information relating to security matters or criminal activities, that is relevant to the exercise of any power or the performance of any duty or function by that Minister under the Citizenship Act or the Immigration and Refugee Protection Act.</li> </ul> </li> </ul>
<b>Croatia</b>	<ul style="list-style-type: none"> <li>• Systematic gathering, analysis, processing and evaluation of information relevant for the national security;</li> <li>• With the aim of detecting and preventing activities, by individuals or groups, directed: against the viability, independence, integrity and sovereignty of the Republic of Croatia, aiming at the violent overthrow of the state authority structures; threatening to violate human rights and basic freedoms established by the Constitution and the legislation of the Republic of Croatia, and to endanger the fundamentals of the economic system of the Republic of Croatia.</li> </ul>
<b>The Netherlands</b>	<ul style="list-style-type: none"> <li>• Conducting investigations regarding organisations that, and persons who, because of the objectives they pursue, or through their activities give cause for serious suspicion that they are a danger to the continued existence of the democratic legal system, or to the security or other vital interests of the state.</li> <li>• Conducting security clearance investigations as referred to in the Security Investigations Act;</li> <li>• Promoting measures [...] for the protection of information that is to remain secret for reasons of national security, and information pertaining to those parts of the public service and business community that in the opinion of the relevant Ministers are of vital importance for the continued existence of the social order;</li> <li>• Conducting investigations regarding other countries concerning subjects designated by the Prime Minister, Minister of General Affairs, in accordance with the relevant Ministers.</li> </ul>

defined as intelligence services that work within the territory of their state, the underlying principles for oversight and control apply equally to intelligence services that operate abroad.

### Intelligence services in a democratic society

#### What is the role of civilian intelligence services in a democratic society?

Intelligence services are an important part of the security sector in a democratic society. Their primary function is to collect and analyse information about threats directed against the state and its population. They provide this information to the government, enabling it to develop and enforce security policy. It is not however, the role of intelligence services to enforce security policy. This is the responsibility of the police and other law enforcement agencies.

The information collection role of intelligence services is limited; their investigations focus only on activities posing a threat to national security. They do this in accordance with legislation and the government's political guidance. Society, not intelligence services, defines what constitutes a threat to national security. This is usually a lengthy process which results in the formulation of a national security policy or legislation.

Intelligence services perform other tasks in addition to their information collection role. For example, they do counter-intelligence activities. These activities include detecting and disrupting espionage conducted by foreign intelligence services that is directed against the interests of the state and its population. Additionally, intelligence services are often responsible for protecting the state's information and information systems. For example, they screen applicants for government jobs that would give those individuals access to classified information. (See Table 1 for details of the mandates and functions of selected intelligence services).

The role of intelligence services is essential for protecting both the state and its population. National law prohibits intelligence services from

promoting or protecting the special interests of any particular religious, ethnic or other group. They remain impartial in their role to serve all individuals in the society. By preventing terrorism and other threats to national security intelligence services contribute to the safety and well being of all individuals in the society.

#### What is the role of military intelligence services?

Military or defence intelligence services are part of the armed forces. In democratic societies, their mandates are more limited than those of civilian intelligence services. They are primarily responsible for collecting and analysing information about threats to armed forces personnel and bases, and for sharing such information with the senior military command and the political leadership. The potential threats that military intelligence services need to monitor may originate from within the armed forces, domestic groups, or from foreign states and entities. In many states, military intelligence services are also tasked with protecting sensitive defence-related information and communication systems. Military intelligence services may operate both domestically and abroad, depending on a country's needs, its legislation, and its force deployment.

Democratic societies do not permit their military intelligence services to gather information about threats to security that are not defence related. Collecting information on non-military threats is the responsibility of civilian intelligence services. Thus, military intelligence services are normally not permitted to collect information on civilians in their own state. In many states, the law requires military intelligence services to call upon the civilian intelligence service if they need to gather information about threats to the armed forces posed by civilians. This restriction is designed to prevent armed forces from interfering in civilian affairs.

# Understanding Intelligence Oversight

## What is the aim of this guidebook?

This guidebook provides an introduction on how democratic states govern their intelligence services. It demonstrates how states can govern their intelligence services in order to make sure that:

- a. They contribute effectively to the security of the state and its population,
- b. They are subject to democratic control,
- c. They are accountable to the populations they serve, and
- d. They respect the rule of law and human rights.

The guidebook provides short and simple answers to frequently asked questions on the activities of intelligence services, as well as the control and oversight of these organisations. It draws extensively on the laws, institutional models and practices of a wide range of democratic states. This guidebook also illustrates that democratic states differ in their approaches to organising, tasking and overseeing their intelligence services. There is no one “right” model or approach. There are however, widely accepted good practices on the activities and oversight of intelligence services which apply in many democratic states – this guidebook outlines many of these.

## What does this guidebook contain?

The guidebook is divided into seven sections. The first focuses on the role intelligence services play in democratic societies. The following section looks at some main features of legal frameworks that regulate intelligence services. Four sections are devoted to explaining how democratic states control the activities of their intelligence services in intelligence collection, the use and management of personal data and international cooperation. The final section of this guidebook focuses on the control and oversight of intelligence services by the executive, parliament, judiciary and expert oversight bodies.

## Who is this guidebook for?

This guidebook is for people interested in the governance of intelligence services, but who do not have an expert understanding of the subject. More specifically, this guidebook addresses three main groups. First, it is for those involved in developing laws and institutions for governing intelligence services. This includes parliamentarians and their staffers, members of the executive, staff from intelligence services, and representatives of civil society organisations. Second, this guidebook is for members and staffers of newly established oversight bodies. Finally, this guidebook hopes to meet the needs of teachers and students who wish to have a general introduction to intelligence governance.

The material in this guidebook is presented in a descriptive way, in the form of a series of simple questions and answers. This format should assist non-expert practitioners in applying and using the material for their own needs.

## What are intelligence services?

This guidebook refers to intelligence services as government organisations, whose main tasks are the collection and analysis of national security related information, and its dissemination to decision makers. This information typically concerns threats to national security such as terrorism, the proliferation of weapons of mass destruction, and espionage by hostile states.

In most democratic states, these tasks are performed by a specialised intelligence service. However, in some countries such tasks are performed by a branch of the police.

States often mandate their intelligence services to work exclusively within or outside the borders of their state. Accordingly, they may have different intelligence services to work at home and abroad. Other states mandate one intelligence service to work both within and outside the national boundaries. While this guidebook focuses primarily on domestic intelligence services,

lawmakers. The toolkit seeks to address this deficiency. One of its aims is to reduce time lawmakers spend on searching for information, thus allowing them to concentrate on their main task. With more information becoming available in Arabic, many citizens and civil society groups may find it easier to articulate their vision of the type of police and security service they want and to contribute to the development of a modern and strong legal framework for the security sector.

### **Why is it important to have a strong legal framework for the security sector?**

A sound legal framework is a precondition for effective, efficient and accountable security sector governance because it:

- Defines the role and mission of the different security organisations;
- Defines the prerogatives and limits the power of security organisations and their members;
- Defines the role and powers of institutions, which control and oversee security organisations;
- Provides a basis for accountability, as it draws a clear line between legal and illegal behaviour;
- Enhances public trust and strengthens legitimacy of government and its security forces.

For all these reasons, security sector reform often starts with a complete review and overhaul of the national security sector legislation. The point is to identify and address contradictions and the lack of clarity regarding roles and mandates of the different institutions.

# Introduction to the Toolkit

Legislating for the security sector is a complex and difficult task. Many lawmakers thus find it tempting to copy legislation from other countries. This expedites the drafting process, especially when the texts are available in the language of the lawmaker, but more often than not, the result is poor legislation.

Even after being amended, the copied laws are often out of date before coming into effect. They may no longer be in line with international standards or they may not fully respond to the requirements of the local political and societal context. Copied laws are sometimes inconsistent with the national legislation in place.

In some cases, there is simply no model law available in the region for the type of legislation that is needed. This has been the case in the Arab region, where the security sector has only slowly begun to be publicly debated. It is thus difficult to find good model laws for democratic policing or for parliamentary oversight of intelligence services.

It is therefore not surprising that many Arab lawmakers have felt frustrated, confused, and overwhelmed by the task of drafting legislation for the security sector. They found it difficult to access international norms and standards because little or no resources were available in Arabic. Many of them did not know where to search for model laws and several were about to give up. Some eventually turned to DCAF for assistance.

The idea of a practical toolkit for legislators in the Arab region came when practitioners began looking for a selection of standards, norms and model laws in Arabic that would help them draft new legislation. Experts from the Arab region and DCAF thus decided to work together and develop some practical tools.

## Who is this toolkit for?

This toolkit is primarily addressed to all those who intend to create new or develop existing security sector legislation. This includes parliamentarians, civil servants, legal experts and nongovernmental organisations. The toolkit may also be helpful to security officials and, as a reference tool, to

researchers and students interested in security sector legislation.

## What is in the toolkit?

The bilingual toolkit contains a number of booklets in English and Arabic that provide norms and standards, guidebooks as well as practical examples of model laws in various areas of security sector legislation.

The following series have been published or are being processed:

- Police legislation
- Intelligence legislation
- Military Justice legislation
- Status of Forces Agreements

Additional series will be added as the needs arise. The existing series can easily be expanded through the addition of new booklets, based on demand from the Arab region.

For the latest status of publications please visit: [www.dcaf.ch/publications](http://www.dcaf.ch/publications)

## What is the purpose of this toolkit?

The toolkit seeks to assist lawmakers in the Arab region in responding to citizens' expectations. Arab citizens demand professional service from police and security forces, which should be effective, efficient and responsive to their needs. They want police and security organisations and their members to abide by the law and human right norms and to be accountable for their performance and conduct. The toolkit thus promotes international standards in security sector legislation, such as democratic oversight, good governance and transparency.

The toolkit offers easy access in Arabic and English to international norms as well as examples of legislation outside the Arab region. This allows to compare between different experiences and practices.

The scarcity of Arab literature on security sector legislation has been a big problem for Arab

## List of Tables and Boxes

<b>Table 1:</b>	Examples of the mandates and functions of intelligence services	12
<b>Table 2:</b>	A comparison of selected intelligence oversight bodies in Belgium, Canada, South Africa and the United Kingdom	35
<b>Box 1:</b>	South African constitutional provisions on the intelligence and security services	13
<b>Box 2:</b>	Extract from Common Article 3 of the Geneva Conventions	16
<b>Box 3:</b>	The process for authorising the use of special powers by the Canadian Security Intelligence Service	20
<b>Box 4:</b>	Regulations on the use of personal data by the German Federal Office for the Protection of the Constitution	23
<b>Box 5:</b>	German law on access to personal data held by intelligence services	24
<b>Box 6:</b>	Croatian regulations on intelligence cooperation with foreign entities	27
<b>Box 7:</b>	International standards on arrest and detention	29
<b>Box 8:</b>	International standards on the use of force by public officials	31
<b>Box 9:</b>	Complaints-handling by Canada's Security Intelligence Review Committee (SIRC)	44
<b>Box 10:</b>	German law on notifying individuals after special powers have been used against them	45

<b>Complaints about intelligence services</b>	<b>43</b>
How can the public complain about intelligence services?	43
Which institutions handle complaints about the intelligence services?	45
Why do some states notify people when special powers have been used against them?	45
What makes a complaints-handling body effective?	46
<b>Further reading</b>	<b>47</b>
<b>Endnotes</b>	<b>48</b>

<b>Internal management</b>	<b>32</b>
What role does internal management play in controlling intelligence services?	32
To whom do intelligence services report?	32
Who appoints directors of intelligence services?	32
Why are directors of intelligence services appointed for a fixed period?	33
<b>The executive</b>	<b>33</b>
What role does the executive play in controlling intelligence services?	33
<b>The judiciary</b>	<b>33</b>
What is the role of the judiciary in controlling and overseeing intelligence services?	33
<b>Parliament</b>	<b>34</b>
What is the role of parliament in controlling and overseeing intelligence services?	34
<b>Expert oversight bodies</b>	<b>34</b>
What is the role of expert intelligence oversight bodies?	34
<b>An in-depth study of parliamentary and expert intelligence oversight bodies</b>	<b>38</b>
Which aspects of intelligence services' work are overseen by parliamentary and/or expert oversight bodies?	38
What legal powers do oversight bodies have?	38
Why do oversight bodies need financial and human resources?	39
How do overseers monitor intelligence services?	39
How do oversight bodies report on their activities?	40
Why are public reports important?	40
Is there a conflict between the right to know and the need to keep information secret?	40
How can the information needs of oversight bodies and intelligence services be reconciled?	40
Why is the relationship between intelligence services and oversight bodies important?	41
How do democratic societies ensure the independence of intelligence oversight bodies?	41
How can the independence of members of oversight bodies be ensured?	42
What are the advantages of parliamentary oversight bodies?	42
What are the advantages of expert oversight bodies?	42

<b>Use and management of personal data</b>	<b>21</b>
What is personal data?	21
How do intelligence services acquire personal data?	21
How do intelligence services and their governments use personal data?	21
Why do democratic societies restrict the use of personal data?	22
What legal controls apply to the use of personal data?	22
Who oversees the use of personal data and what do they do?	23
Can individuals access their personal data?	24
<b>International intelligence cooperation</b>	<b>25</b>
What is international intelligence cooperation?	25
Why do intelligence services cooperate with foreign governments and intelligence services?	25
What are the risks of intelligence cooperation?	25
How do states control international intelligence cooperation?	26
What controls apply to the sharing of information with foreign intelligence services?	26
How is international intelligence cooperation overseen?	27
<b>The intelligence services' use of powers of arrest and detention</b>	<b>27</b>
Should intelligence services have powers to arrest and detain individuals?	27
What international standards apply to the use of powers of arrest and detention?	28
Do intelligence services need their own detention facilities?	28
<b>The use of lethal force by intelligence services</b>	<b>28</b>
Are intelligence services permitted to kill?	28
<b>The control and oversight of intelligence services</b>	<b>31</b>
Why do democratic societies control their intelligence services?	31
Which institutions control and/or oversee intelligence services?	32

# TABLE OF CONTENTS

<b>Introduction to the Toolkit</b>	<b>8</b>
<b>Understanding Intelligence Oversight</b>	<b>10</b>
What is the aim of this guidebook?	10
What does this guidebook contain?	10
Who is this guidebook for?	10
What are intelligence services?	10
<b>Intelligence services in a democratic society</b>	<b>11</b>
What is the role of civilian intelligence services in a democratic society?	11
What is the role of military intelligence services?	11
<b>Legal framework for intelligence services</b>	<b>13</b>
How do democratic societies provide a legal basis for intelligence services?	13
Why do intelligence services need a legal basis?	13
Are intelligence laws secret?	14
What do intelligence laws cover?	14
How do democratic societies ensure intelligence services uphold the law?	15
What are the international legal standards guiding intelligence services?	15
Are intelligence services permitted to violate human rights?	15
<b>Information collection</b>	<b>17</b>
How do intelligence services collect information?	17
What information are intelligence services permitted to collect?	17
What information are intelligence services not permitted to collect?	18
Why do states restrict the collection of information from certain professions?	18
How does a democratic society control the use of special powers?	18
Who authorises the use of special powers?	18
How does the state authorise the use of special powers?	19
How do democratic societies oversee the use of special powers?	19

## About DCAF

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) promotes good governance and reform of the security sector. The Centre conducts research on good practices, encourages the development of appropriate norms at the national and international levels, makes policy recommendations and provides in-country advice and assistance programmes. DCAF's partners include governments, parliaments, civil society, international organisations and security sector actors such as police, judiciary, intelligence agencies, border security services and the military.

Further information on DCAF is available at:  
[www.dcaf.ch](http://www.dcaf.ch)

## Acknowledgements

DCAF would like to thank the members of the Editorial Board for their dedication and the time they devoted to review this series.

Furthermore, DCAF would like to thank Beverly Youmans and Stephanie Chaban for their editorial assistance.

## Publisher

Geneva Centre for Democratic Control of Armed Forces (DCAF).

Cover picture © REUTERS/ Chris Wattie, 2007

ISBN: 978-92-9222-131-7

© DCAF 2010. All rights reserved.

## Editorial Board

The Editorial Board for the series of booklets on intelligence oversight comprises:

- Hans Born, Geneva
- Ian Leigh, Durham
- Arnold Luethold, Geneva
- Benjamin Buckland, Geneva

Guidebook

# Understanding Intelligence Oversight

Aidan Wills





Guidebook

# Understanding Intelligence Oversight

Aidan Wills



Geneva Centre for the  
Democratic Control of  
Armed Forces (DCAF)