

## Recommandations pour le cadre législatif grec en matière de surveillance

November 2022

### Résumé des recommandations

#### 1. Absence de contrôle judiciaire dans les cas de surveillance pour des raisons de sécurité nationale

- Permettre un contrôle judiciaire indépendant des demandes de surveillance par les services de sécurité et une autorité judiciaire indépendante pour autoriser les demandes, y compris dans les cas d'atteinte présumée à la sécurité nationale.
- Contraindre les forces de sécurité à justifier la demande de surveillance afin qu'un contrôle judiciaire permette de déterminer sa conformité avec les principes de légalité, de nécessité et de proportionnalité.
- S'assurer non seulement de l'indépendance, mais aussi de l'efficacité du contrôle, de la nécessité et de la proportionnalité de la demande de surveillance.
- Abroger le récent amendement à la loi empêchant les personnes d'être informées du fait qu'elles étaient soumises à une surveillance, afin qu'elles puissent exercer leur droit à un recours effectif.

#### 2. Absence de garanties contre l'abus de surveillance

- Prévoir une limitation proportionnée de la période pendant laquelle une personne peut être placée sous surveillance pour des raisons de sécurité nationale, conformément à la jurisprudence de la CEDH.
- Limiter légalement les types de communications pouvant être interceptées et les moyens par lesquels ces interceptions peuvent être effectuées.
- S'assurer que les informations recueillies correspondent uniquement à la perpétration ou la préparation présumée d'un crime.
- Prévoir une procédure de destruction des données récoltées lorsque les enquêtes sur une atteinte présumée à la sécurité nationale ne confirment pas ces allégations, sous le contrôle d'une autorité indépendante ou judiciaire.

#### 3. Absence de garanties spécifiques contre la surveillance de journalistes

- Prévoir des garanties spécifiques dans les cas de demande de surveillance d'un journaliste : protection des sources journalistiques, renforcement du contrôle judiciaire, protection contre la surveillance accidentelle.

#### 4. Absence d'un cadre législatif suffisant sur l'utilisation de logiciels espions

- Transparence sur l'utilisation de logiciels espions.
- Conformité de l'utilisation de logiciels espions avec les garanties énoncées plus haut.

#### 5. Définition floue de sécurité nationale

- Revoir la législation sur la sécurité nationale, pour s'assurer que les conditions permettant la surveillance pour cette raison répondent aux exigences de légitimité, de nécessité et de prévisibilité.
- Au minimum, la législation doit définir ce qui constitue une atteinte à la sécurité nationale et fournir une définition des catégories de personnes susceptibles d'être considérées comme une menace à la sécurité nationale, ainsi que les objets pouvant être placés sous surveillance.

Les cas récents d'espionnage de deux journalistes en Grèce, Thanasis Koukakis et Stavros Malichudis, ont révélé d'inquiétantes insuffisances dans le cadre législatif grec en matière de surveillance, et l'absence de garanties quant au respect des droits humains et des libertés journalistiques, au regard des normes internationales et de la jurisprudence de la Cour européenne des droits de l'homme (CEDH). Il s'agit en particulier de l'absence d'un contrôle judiciaire suffisant et de l'absence de garanties spécifiques contre la surveillance de journalistes sur la base du droit au secret des sources. Ces inquiétudes ont été renforcées par la révélation, en octobre 2022, de l'espionnage présumé, *via* leurs téléphones, des déplacements de Thanasis Koukakis et de trois autres journalistes enquêtant sur le scandale de surveillance.

La CEDH, dans un récent arrêt relatif à la question de l'atteinte à la confidentialité des communications des personnes pour raison de sécurité nationale, a considéré que **six "garanties minimales"** devaient être établies par la loi pour éviter les abus de pouvoir dans l'interception de communications dans le cadre d'enquêtes pénales : "i) *la nature des infractions susceptibles de donner lieu à un mandat d'interception ; ii) la définition des catégories de personnes dont les communications sont susceptibles d'être interceptées ; iii) la limitation de la durée d'exécution de la mesure ; iv) la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies ; v) les précautions à prendre pour la communication des données à d'autres parties ; et vi) les circonstances dans lesquelles les données interceptées peuvent ou doivent être effacées ou détruites.*"<sup>1</sup>

Dans les cas concernant la sécurité nationale, bien que la Cour ait reconnu que "**les autorités nationales disposent d'une ample marge d'appréciation pour choisir les moyens de sauvegarder au mieux la sécurité nationale**"<sup>2</sup>, elle a considéré que "ces mêmes garanties minimales, au nombre de six, s'appliqu[ai]ent aussi dans les cas où l'interception [était] faite pour des raisons de sécurité nationale"<sup>3</sup>. Elle a ajouté, dans ces cas de sécurité nationale, **trois garanties supplémentaires** à respecter, "compte tenu du risque qu'un système de surveillance secrète destiné à protéger la sécurité nationale pourrait saper, voire détruire, les processus démocratiques sous couvert de les défendre"<sup>4</sup> : la Cour "prend également en considération les modalités de contrôle de la mise en œuvre des mesures de surveillance secrète, les mécanismes de notification et les voies de recours prévues par le droit national"<sup>5</sup>.

Les points ci-dessous démontreront que ces **neuf garanties exigées par la CEDH, qui sont des garanties minimales, sont inexistantes ou très insuffisantes dans la loi grecque**, en particulier les garanties concernant les procédures d'autorisation de surveillance, la prévisibilité des motifs de l'autorisation, l'existence de recours, ainsi que la nature, la portée et la durée de la surveillance.

Reporters sans frontières (RSF) appelle les autorités grecques à inscrire ces garanties dans la loi afin que son cadre législatif sur le droit à la vie privée et les libertés journalistiques répondent aux normes internationales des droits humains.

## 1. Absence de contrôle judiciaire dans les cas de surveillance opérée pour des raisons de sécurité nationale

### ● Absence d'autorisation judiciaire indépendante

Dans les cas n'impliquant *pas* la sécurité nationale, les demandes des services de sécurité de porter atteinte à la confidentialité des communications d'une personne doivent être acceptées par un panel de trois juges.

---

<sup>1</sup> Affaire Big Brother Watch et autres c. Royaume-Uni, § 335 - <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%2201-210280%22%7D>

<sup>2</sup> *ibid*, § 338.

<sup>3</sup> *ibid*.

<sup>4</sup> *ibid*, § 339.

<sup>5</sup> *ibid*, § 338

La procédure est complètement différente dans les cas de menace présumée à la sécurité nationale : la demande des services de sécurité de porter atteinte à la confidentialité d'une communication d'une personne n'est pas soumise à un juge, mais à un procureur spécial, qui ne peut être considéré comme une autorité judiciaire indépendante.

Bien qu'une loi, disposant que non plus un mais deux procureurs doivent désormais autoriser la surveillance, ait récemment été adoptée, cela reste insuffisant.

Cette procédure spéciale applicable dans les cas de sécurité nationale entre en contradiction avec les garanties préconisées par la CEDH. La Cour, en effet, a décidé que :

*“En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le contrôle judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière.”<sup>6</sup>*

Dans un autre arrêt, la Cour a considéré que le fait que des autorités compétentes doivent demander une autorisation judiciaire pour la surveillance “est une garantie importante contre l'arbitraire et les abus”, car cela “peut limiter leur pouvoir d'interprétation de cette notion (de sécurité nationale) et assurer que des raisons suffisantes de placer une personne sous surveillance sont présentes dans chaque cas”.<sup>7</sup>

⇒ La législation grecque doit permettre un contrôle judiciaire indépendant des demandes de surveillance émises par les services de sécurité, et à une autorité judiciaire indépendante d'autoriser de telles demandes, y compris dans les cas d'atteinte présumée à la sécurité nationale.

⇒ La législation grecque devrait également contraindre les forces de sécurité à justifier la demande de surveillance, afin qu'un contrôle judiciaire puisse évaluer si elle est conforme avec les principes de légalité, de nécessité et de proportionnalité.

- **Impossibilité d'un contrôle effectif de la nécessité et de la proportionnalité de la surveillance**

Lorsque la surveillance d'une personne est demandée pour des raisons de sécurité nationale, la demande au procureur ne nécessite pas de préciser les motivations de la surveillance, empêchant le procureur d'évaluer si la surveillance demandée répond aux exigences de nécessité et de proportionnalité, et d'évaluer si la surveillance doit se poursuivre ou cesser.

Cela entre en contradiction directe avec la jurisprudence de la CEDH selon laquelle la surveillance doit répondre aux principes de nécessité et de proportionnalité. En effet, la Cour énonce :

*“Afin de constituer une garantie effective contre les abus, l'organe indépendant chargé d'accorder les autorisations devrait être **informé à la fois du but poursuivi par l'interception et des canaux de transmission ou des voies de communication susceptibles d'être interceptés.** Cela lui permettrait d'apprécier la nécessité et la proportionnalité de l'opération d'interception en masse ainsi que de vérifier si la sélection des canaux est nécessaire et proportionnée aux buts dans lesquels les activités d'interception sont menées.”<sup>8</sup>*

⇒ La législation grecque doit s'assurer non seulement de l'indépendance, mais aussi de

<sup>6</sup> *ibid*, § 336.

<sup>7</sup> CEDH, *Ekimdzhev et autres c. Bulgarie*, 2022, § 301 - <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-214673%22%7D>

<sup>8</sup> *Affaire Big Brother Watch et autres c. Royaume-Uni*, *op. cit.*, § 352.

**l'effectivité du contrôle de la nécessité et de la proportionnalité de la surveillance demandée.**

- **Absence de contrôle judiciaire après que la surveillance a pris fin; violation du droit à un recours effectif**

Après le cas Koukakis, le loi grecque a été revue de manière à ne plus permettre, d'aucune façon, qu'une personne concernée par une surveillance soit informée de ladite surveillance lorsqu'elle a pris fin, même dans les cas où la surveillance n'a pas confirmé la suspicion d'atteinte à la sécurité nationale.

Il est à noter qu'avant ce récent amendement, l'Autorité hellénique pour la sécurité et la confidentialité des communications (ADAE) pouvait notifier à la personne lésée l'arrêt de la surveillance, que ce soit à des fins d'enquête pour acte criminel grave ou pour des raisons de sécurité nationale.

Cela rend impossible l'exercice d'un contrôle judiciaire sur la surveillance, afin de s'assurer qu'elle est conforme aux exigences de légalité et de nécessité. La CEDH a pourtant considéré que *"le contrôle et la supervision des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé"*.<sup>9</sup> En ce qui concerne le troisième stade, après que la surveillance est terminée, la Cour énonce :

*"La question de la notification a posteriori de mesures de surveillance est un facteur pertinent pour apprécier l'effectivité des recours judiciaires et donc l'existence de garanties efficaces contre les abus des pouvoirs de surveillance."*<sup>10</sup>

Ce récent amendement à la loi constitue ainsi une violation du droit à un recours effectif pouvant être exercé contre une surveillance abusive.

**⇒ Les autorités grecques doivent abroger, avec effet rétroactif, le récent amendement à la loi qui empêche les personnes d'être informées du fait qu'elles ont fait l'objet d'une surveillance, afin de s'assurer qu'elles peuvent exercer leur droit à un recours effectif.**

## 2. Absence de garanties contre l'abus de surveillance

- **Lack of limitation of the period of surveillance**

L'article 5 de la loi n° 2225/1994 ne prévoit pas de période maximum durant laquelle la surveillance peut être effectuée dans les cas de sécurité nationale – contrairement aux cas d'enquêtes sur un délit, où la limite maximum est de 10 mois.

L'absence de limitation constitue une violation de la jurisprudence de la CEDH. La Cour, dans un arrêt faisant référence à la limite de deux ans maximum pour la surveillance prévue par la loi bulgare, a exprimé le point de vue que *"la longue durée de cette période, associée aux contours intrinsèquement flous de la notion de sécurité nationale, affaiblit significativement le contrôle judiciaire auquel une telle surveillance doit être soumise"*.<sup>11</sup>

C'est a fortiori le cas en Grèce, où aucune limite de temps n'est prévue pour les cas de sécurité nationale.

<sup>9</sup> *ibid*, § 336.

<sup>10</sup> *ibid*, § 337.

<sup>11</sup> CEDH, Ekimdzhev et autres c. Bulgarie, 2022, § 305 - <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-214673%22%5D%7D>

⇒ **La législation grecque doit prévoir une limitation proportionnée de la période durant laquelle une personne peut être placée sous surveillance pour des raisons de sécurité nationale, en conformité avec la jurisprudence de la CEDH.**

- **Absence de spécifications du type de communications pouvant être interceptées et des moyens d'interception**

La législation grecque sur la surveillance secrète de citoyens pour des raisons de sécurité nationale ne précise pas les types de communication pour lesquelles la levée du secret peut être demandée, telle que les adresses IP ou les communications électroniques. L'article 5-1 de la loi n° 2225/1994 énonce simplement que les ordres d'interception doivent préciser les types de communications pouvant être interceptées, laissant à l'autorité en charge toute latitude pour décider d'intercepter tout type de communication, sans limitation.

La loi ne précise pas non plus les moyens par lesquels l'interception peut être demandée.

Cette absence de spécifications accorde un pouvoir trop étendu aux forces de sécurité et constitue une violation des principes de nécessité et de proportionnalité exigés par la Convention européenne.

⇒ **La loi doit limiter juridiquement les types de communications pouvant être interceptées et les moyens par lesquels cette interception peut être réalisée.**

- **Absence de limitation sur les informations pouvant être recueillies**

Dans le cas de Stavros Malichudis, il a été révélé que les informations recueillies à son propos ne concernaient aucune atteinte à la loi, mais étaient liées à ses affiliations politiques, ses activités journalistiques, etc.

Cela confirme que l'absence de contrôle judiciaire et de limitations suffisantes dans la loi permettent d'effectuer une surveillance abusive, soit une violation du principe de *"nécessité dans une société démocratique"* prévue par la CEDH.

⇒ **La loi grecque doit s'assurer que les informations recueillies se limitent à celles correspondant à une perpétration ou une préparation présumée d'un crime.**

- **Absence de dispositions permettant la destruction des données collectées**

L'article 5 de la loi n° 2225/1994 n'inclut aucune procédure concernant la destruction des données collectées dans le cadre d'une procédure de sécurité nationale dans les cas où les enquêtes n'ont pas confirmé les suspicions d'atteinte à la sécurité nationale – contrairement aux cas où les enquêtes ne concernent pas la sécurité nationale, où les données en question sont détruites si elles ne constituent pas des preuves.

La loi ne permet pas non plus à une autorité compétente de prendre en charge le stockage et la préservation de ces données.

⇒ **La loi grecque doit prévoir une procédure de destruction des données collectées lorsque les enquêtes sur une atteinte présumée à la sécurité nationale n'ont pas confirmé ces allégations.**

⇒ Une telle procédure doit être exécutée sous le contrôle d'une autorité indépendante ou d'une autorité judiciaire.  
⇒ Les personnes doivent avoir le droit d'être informées de cette destruction, et de faire appel à un juge pour s'assurer que la destruction a bien été effectuée.

### 3. Absence de garanties spécifiques contre la surveillance de journalistes

Étant donné leur fonction sociale consistant à informer le public sur les questions d'intérêt général et de suivre les actions des autorités publiques, les journalistes doivent bénéficier de droits particuliers, et notamment la protection du secret des sources. À cet égard, la CEDH a jugé à maintes reprises que :

*“Les garanties à accorder à la presse revêtent une importance particulière, et la protection des sources journalistiques est l'une des pierres angulaires de la liberté de la presse. L'absence d'une telle protection pourrait dissuader les sources journalistiques d'aider la presse à informer le public sur des questions d'intérêt général. En conséquence, la presse pourrait être moins à même de jouer son rôle indispensable de 'chien de garde' et son aptitude à fournir des informations précises et fiables pourrait s'en trouver amoindrie.”<sup>12</sup>*

La surveillance de journalistes est particulièrement inquiétante du fait qu'elle peut “avoir un impact préjudiciable non seulement sur les sources, dont l'identité peut être révélée, mais également sur le journal ou toute autre publication visés par l'injonction, dont la réputation auprès des sources potentielles futures peut être affectée négativement par la divulgation, et sur les membres du public, qui ont un intérêt à recevoir les informations communiquées par des sources anonymes.”<sup>13</sup>

La surveillance de journalistes est, par nature, à même de constituer une violation du secret des sources. La Cour considère ainsi que :

**“Toute atteinte au droit à la protection des sources journalistiques doit être entourée de garanties procédurales, définies par la loi, en rapport avec l'importance du principe en jeu. Au premier rang des garanties exigées doit figurer la possibilité de faire contrôler la mesure par un juge ou tout autre organe décisionnel indépendant et impartial investi du pouvoir de dire s'il existe un impératif d'intérêt public l'emportant sur le principe de protection des sources des journalistes et, dans le cas contraire, d'empêcher tout accès non indispensable aux informations susceptibles de conduire à la divulgation de l'identité des sources.”**

*“Eu égard à la nature préventive d'un tel contrôle de, le juge ou tout autre organe indépendant et impartial doit donc être en mesure d'effectuer, avant toute divulgation, cette mise en balance des risques potentiels et des intérêts respectifs relatifs aux éléments dont la divulgation est demandée. Cela afin que les arguments des autorités désireuses d'obtenir la divulgation puissent être correctement appréciés. La décision à prendre doit être régie par des critères clairs, notamment celui de savoir si une mesure moins intrusive peut suffire à servir l'intérêt public supérieur établi. Le juge ou tout autre organe compétent doit avoir la faculté de refuser de délivrer une injonction de divulgation ou d'émettre une injonction de portée plus limitée ou plus encadrée, de manière à ce que les sources concernées puissent échapper à la divulgation de leur identité, qu'elles soient ou non spécifiquement nommées dans les pièces dont la remise*

<sup>12</sup> Affaire Goodwin c. Royaume-Uni, 1996, § 39 - [https://hudoc.echr.coe.int/fre#%22itemid%22:\[%22001-62533%22\]](https://hudoc.echr.coe.int/fre#%22itemid%22:[%22001-62533%22])

<sup>13</sup> Affaire Big Brother Watch et autres c. Royaume-Uni, *op. cit.*, § 443.

*est demandée, au motif que la communication de telles pièces créerait un risque sérieux de compromettre l'identité de sources de journalistes.*<sup>14</sup>

L'arrêt renforce clairement l'argument de RSF selon lequel la surveillance, même dans des cas de sécurité nationale, doit être soumise à un contrôle judiciaire préalable et continu. Ce contrôle doit être renforcé dans les cas impliquant un journaliste.

⇒ **La loi grecque doit prévoir des garanties spécifiques dans les cas de demande de surveillance d'un journaliste. Ces garanties doivent prévoir, en particulier :**

- **l'obligation de l'autorité qui émet la demande de démontrer que la surveillance ne vise pas à identifier les sources du journaliste, sauf s'il est démontré qu'il existe une exigence impérieuse d'intérêt public, en conformité avec la jurisprudence de la CEDH ;**
- **le renforcement et la continuité d'un contrôle judiciaire indépendant d'une surveillance impliquant un journaliste ;**
- **que lorsque la surveillance d'un journaliste est autorisée par une autorité judiciaire indépendante, cette autorité doit s'assurer que la surveillance et les données collectées sont strictement limitées par les motifs de l'autorisation et ne débordent pas sur des informations sans lien avec ces motifs, en particulier des informations relatives à l'activité journalistique ou au secret des sources ;**
- **qu'une surveillance indirecte ou accidentelle d'un journaliste (lorsque le journaliste n'est pas lui-même l'objet de la surveillance, mais est en contact avec une personne qui est l'objet direct de cette surveillance) doit immédiatement nécessiter un contrôle judiciaire et une autorisation spécifiques, afin de s'assurer que les informations confidentielles relatives à l'activité du journaliste ou de ses sources ne sont pas recueillies.**

#### 4. Absence de cadre législatif suffisant pour l'utilisation de logiciels espions

L'affaire Koukakis a révélé que le logiciel espion Predator avait été utilisé contre le journaliste – alors même que l'utilisation de logiciels espions n'est pas autorisée par la loi et est donc illégale.

L'utilisation de logiciels espions – bien qu'ils puissent être des outils efficaces pour lutter, par exemple, contre le crime organisé, le trafic de drogue ou le terrorisme – peut constituer une violation grave du droit à la vie privée et des droits des journalistes. Ainsi, elle doit être explicitement prévue et strictement réglementée par la loi.

Ces garanties contre l'utilisation de tels outils technologiques existent bien dans la loi grecque, mais sont trop faibles. Par exemple, et comme énoncé plus haut, la législation grecque ne précise pas les moyens par lesquels une surveillance peut être effectuée, ce qui permet aux autorités d'utiliser tous les moyens jugés nécessaires, aussi disproportionnés soient-ils.

⇒ **La législation grecque doit contraindre les autorités exécutives à révéler et à débattre publiquement de l'utilisation de tels logiciels, de l'acquisition de tels logiciels ou de l'utilisation d'intermédiaires pour effectuer une surveillance à travers l'utilisation de tels logiciels.**

⇒ **La loi doit être claire sur le fait que lorsque la surveillance n'est pas possible en vertu de la loi, l'utilisation d'un logiciel espion n'est pas possible non plus.**

<sup>14</sup> *ibid*, § 444 et 445.

⇒ Les mêmes exigences, telles que citées dans ce document (nécessité, proportionnalité, contrôle judiciaire indépendant, limitations, etc.), doivent s'appliquer lorsque la surveillance est effectuée à travers l'utilisation de logiciels espions, y compris *via* des intermédiaires.  
⇒ Les mêmes garanties vis-à-vis des journalistes doivent s'appliquer lorsque la surveillance est effectuée avec un logiciel espion.

## 5. Définition vague de sécurité nationale

Les menaces à la sécurité nationale autorisent des atteintes à la confidentialité des communications selon la loi grecque – ainsi que l'autorisent les normes internationales et la Convention européenne des droits humains (article 8). Toutefois, la loi ne prévoit pas de définition de "sécurité nationale" ou d'"atteinte à la sécurité nationale". Les articles 3 et 5 de la loi n° 2225/1994, qui établissent la procédure pour la levée de la confidentialité pour des raisons de sécurité nationale, ne font aucune mention des catégories de personnes pouvant être considérées comme une menace à la sécurité nationale. Ils autorisent une atteinte à la confidentialité des communications de n'importe quel citoyen, et ne prévoient aucune procédure pour s'opposer à cette atteinte.

Cette absence de définition et de clarté entre en contradiction avec la jurisprudence de la CEDH, qui énonce que toute ingérence dans le droit d'une personne à la vie privée ne peut être justifiée que si elle est conforme à la loi, qu'elle poursuit un objectif légitime selon l'article 8-2 de la Convention (parmi lesquels la sécurité nationale) et qu'elle est nécessaire dans une société démocratique afin d'atteindre cet objectif. La Cour a insisté sur le fait que la loi autorisant une telle ingérence doit être "prévisible" :

*"En matière de surveillance secrète, la 'prévisibilité' ne peut se comprendre de la même façon que dans la plupart des autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la 'prévisibilité' ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles de recourir à ce type de mesures de manière à ce qu'il puisse adapter sa conduite en conséquence. Cependant, le risque d'arbitraire est évident lorsqu'un pouvoir dévolu à l'exécutif s'exerce en secret. Il est donc indispensable de disposer de règles claires et détaillées en matière de mesures de surveillance secrète (...). Le droit interne doit être suffisamment clair pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions la puissance publique est habilitée à recourir à pareilles mesures."*<sup>15</sup>

La condition de prévisibilité ne peut être considérée comme remplie lorsque les raisons qui ont autorisé une atteinte à la confidentialité des communications d'une personne ne sont pas suffisamment définies.

⇒ Les autorités grecques doivent revoir la législation sur la sécurité nationale, afin de s'assurer que les conditions de la surveillance pour cette raison répondent aux exigences de légitimité, de nécessité et de prévisibilité.  
⇒ Au minimum, la législation doit définir ce qui constitue une atteinte à la sécurité nationale et prévoir une définition des catégories de personnes pouvant être considérées comme une menace à la sécurité nationale, et les objets pouvant être placés sous surveillance.

<sup>15</sup> *ibid*, § 333.

**Pour plus d'information :**

Paul Coppin, assistant du responsable plaidoyer, responsable juridique à Reporters sans frontières  
[paul.coppin@rsf.org](mailto:paul.coppin@rsf.org)