Avril
2016

ÉVALUATION ET PERSPECTIVES DES MENACES SÉCURITAIRES

Rapport de synthèse pour

le Forum Technology against Crime (TAC), édition 2016.

Edité par Jean-Pierre Maulny et Sabine Sarraf, IRIS

Évaluation et perspectives des menaces sécuritaires

Rapport de synthèse pour le Forum Technology against Crime (TAC), édition 2016.

Le rapport présente une analyse croisée et comparative des approches nationales en matière de sécurité et, au-delà, envisage les convergences européennes possibles. Son objet consiste à évaluer la menace sécuritaire au cours des prochaines décennies et à apprécier la manière dont les nouvelles technologies peuvent constituer un défi et une réponse à leur apporter. Sont également listés dans cette étude divers instruments juridiques, existants ou pouvant être envisagés, afin de restreindre la potentialité des risques. Toutes ces dimensions sont observées dans la perspective des débats sociétaux qui y sont corrélés. Quatre questions sont donc abordées successivement :

- De quelle manière les menaces sécuritaires vont-elles évoluer au cours des prochaines décennies ? [3]
- De quelle manière les nouvelles technologies peuvent-elles constituer une réponse aux menaces sécuritaires ? [8]
- Quelles seraient les dispositions législatives susceptibles d'apporter des réponses à ces menaces ? [12]
- Quels sont les débats publics, existants ou futurs, pouvant influencer les mesures de lutte contre la menace sécuritaire ? [20]

Edité par Jean-Pierre Maulny et Sabine Sarraf, IRIS

Contributeurs :

Felix Arteaga, Institut Royal Elcano (*Real Instituto Elcano*), *Espagne*
Caroline Baylon, Chatham House et le Centre de recherche de décisions stratégiques, *Grande-Bretagne*
Eline Chivot, Centre d'études stratégiques de La Haye (HCSS), *Pays-Bas*
Anja Dahlmann, Institut allemand des affaires internationales et stratégiques (*Stiftung Wissenschaft und Politik*, SWP), *Allemagne*
Marcel Dickow, Institut allemand des affaires internationales et stratégiques (*Stiftung Wissenschaft und Politik*, SWP), *Allemagne*
Artur Kacprzyk, Institut polonais des affaires internationales (*Polski Instytut Spraw Międzynarodowych*, PISM), *Pologne*
Alessandro Marrone, Institut des affaires internationales (*Istituto Affari Internazionali*, IAI), *Italy*
Jean-Pierre Maulny, Institut de relations internationales et stratégiques (IRIS), *France*
Rui Carlos Pereira, Observatoire sur la sécurité publique, le crime organisé et le terrorisme (*Observatório de Segurança, Criminalidade Organizada e Terrorismo*, OSCOT), *Portugal*
Sabine Sarraf, Institut de relations internationales et stratégiques (IRIS), *France*

DE QUELLE MANIÈRE LES MENACES SÉCURITAIRES VONT-ELLES ÉVOLUER AU COURS DES PROCHAINES DÉCENNIES ?

La définition de ce que peut être une menace sécuritaire est subjective et évolutive. Elle dépend du point de vue à partir duquel on la détermine. On constate que les différents pays n'abordent pas la sécurité de la même manière. Tandis que **la France** et **les Pays-Bas**, privilégient une approche en fonction de l'objectif de sécurité recherché, tel que la protection du territoire, la stabilité économique ou la sécurité sanitaire, les autres pays contributeurs s'intéressent à la sécurité en partant de la menace constatée. De ce fait, Néerlandais et Français estiment que la sécurité couvre un champ d'hypothèses plus large, prenant en compte les menaces non intentionnelles comme des grandes catastrophes naturelles ou des défaillances techniques. C'est une définition exhaustive qui n'exclut pas une priorisation des menaces, même si cet exercice n'est pas nécessairement codifié dans un texte. Mais la majeure partie des pays entend la sécurité au sens de sûreté, c'est à dire de lutte contre une intention ou un acte de malveillance.

L'Allemagne et le Royaume-Uni, de leur côté, envisagent expressément la sécurité sous les aspects de la sécurité publique et individuelle. Ils rassemblent sous la première expression les principaux objectifs devant être atteints, ceux de prévention du risque terroriste et de la grande criminalité, la protection des infrastructures critiques et vitales ou encore, par exemple, la cybercriminalité. Concernant la sécurité individuelle, les auteurs relèvent l'importance des atteintes à la vie privée ou tous les droits liés au traitement de données à caractère personnel et à la surveillance de masse.

Avant même de prioriser les menaces à leur sécurité, tous **les États mettent en avant le fait qu'il existe une disparition progressive de la frontière entre sécurité extérieure et sécurité intérieure**. Les menaces de sécurité extérieure deviennent des menaces de sécurité intérieure, et celles-ci prennent aujourd'hui le pas sur les menaces « classiques » que sont la délinquance et la criminalité. L**'Espagne** donne une cause structurelle à cette évolution**.** Pour ce pays, la mondialisation joue un rôle important dans l'évolution de l'environnement sécuritaire. Cela se traduit par une dématérialisation des frontières qui augmente « la surface d'attaque créant des imprévisibilités quant à la source, l'origine territoriale de la menace de sécurité ». Les acteurs non-étatiques peuvent opérer au-delà des frontières, effaçant la distinction traditionnelle entre sécurité intérieure et extérieure, contraignant ainsi les forces de l'ordre de différents pays à coopérer pour agir efficacement à l'échelle supranationale.

Pour d'autres pays, les deux notions de sécurité intérieure et extérieure s'effacent même complètement. En Pologne, on constate que les principaux risques en matière de cyber sécurité portent ur des actions conduites, financées et encouragées par des acteurs résidants en dehors de son territoire, que ce soit des unités de cybercriminalité ou des groupes publics de hackers. La réponse à ces activités relèvent principalement de la compétence des agences de sécurité intérieure, notamment si les systèmes attaqués

concernent des infrastructures critiques tels que les réseaux publics de communication, les réseaux d'approvionnement en électricité ou les systèmes de gestion des transports. Abordé directement au prisme d'une résurgence perçue de la menace russe. Pour un grand nombre de pays, à commencer par la France, le terrorisme international et transfrontalier est devenu la menace principale en 2015

S'il existe bien une *priorisation* des menaces, celle-ci est souvent implicite et ne résulte pas d'une politique de sécurité intérieure qui globaliserait l'action des États dans ce domaine.

Ainsi, en 2015 **l'Allemagne** s'est concentrée sur les atteintes pouvant être portées aux libertés individuelles, notamment celles liées à la protection des données à caractère personnel et au respect de la vie privée, ceci du fait de l'extrême sensibilité de la société allemande sur ces questions. Elle met également en avant les questions de cyber sécurité ou d'approvisionnement énergétique et en minerais, deux domaines qui ont chacun fait l'objet récemment d'une nouvelle stratégie (2015 pour le premier, 2016 pour le second), et sont notamment liées aux craintes en matière de protection des infrastructures vitales[1].

D'une manière générale, le cyberespace fait face à un phénomène de prolifération d'outils malveillants dont l'appréhension est particulièrement complexe. Il est communément admis que la menace de cyber sécurité est une priorité difficile à cerner, et s'apprécie différemment selon les États. L'Allemagne met en avant les atteintes possibles aux libertés individuelles liées au développement du cyber, mais les Allemands font aussi le lien entre terrorisme, menaces d'États tiers et cyber attaques. La **Pologne** lie beaucoup plus directement la menace cyber à la menace extérieure, compte-tenu du fait qu'une large majorité des cyberattaques ont une origine extérieure au territoire du pays attaqué. La Pologne s'inquiète d'un usage du cyberespace à des fins d'espionnage, d'opérations militaires ou d'actes de terrorisme, que ce soit par des acteurs étatiques ou non étatiques.

Au Royaume-Uni, le cyber est également considéré comme la menace principale, et ce quelle que soit son origine. Du point de vue britannique, c'est la multiplicité des effets possibles, c'est-à-dire des cibles potentielles d'une cyber attaque, qui constitue la menace. Sont ainsi énumérées les attaques sur les infrastructures ou le système bancaire, le déni d'accès à internet, la possibilité d'attaquer des réseaux non connectés qui commencent à se développer, et les atteintes aux diverses libertés publiques et à la vie privée.

Par ailleurs, les objectifs des attaques peuvent être divers dans leur nature. Il peut s'agir d'espionnage opéré par des acteurs étatiques. Il peut s'agir de paralyser un pays en

[1] Cf. German Ministry of the Interior, *Cyber Security Strategy for Germany* (February 2011), retrieved 12.10.2015, at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.html ; and German Government, *The German Government's Raw Materials Strategy* (October 2010), retrieved 18.01.2016, at http://www.bmwi.de/English/Redaktion/Pdf/raw-materials-strategy,property=pdf,bereich=bmwi2012,sprache=en,rwb=true.pdf

visant ses infrastructures vitales. Il peut enfin s'agir de frapper la sphère politique ou l'économie d'un pays, par exemple en s'attaquant à une industrie aux activités essentielles à la survie de l'État. La cyber-menace en provenance d'acteurs non étatiques est encore plus difficile à appréhender. Elle est presque imprévisible car elle ne repose pas sur des tendances diplomatiques connues, contrairement à celles établies d'État à État.

Pour l'**Italie**, l'ordre des menaces place le terrorisme au sommet des priorités, suivi de la question migratoire et de la menace cyber. La perception de la question migratoire par l'Italie est intéressante, car ce phénomène se traduit en menaces potentielles ou avérées qui sont au nombre de trois : le terrorisme, la question de l'ordre public lié au phénomène de congestion des centres dédiés aux migrants, ainsi que les opportunités offertes à la criminalité organisée à travers le trafic d'êtres humains.

Le terrorisme figure également en tête de liste des menaces sécuritaires pour l'**Espagne**, avec le risque cyber et le crime organisé. Dans ce pays, il est moins fait référence au phénomène migratoire, mais cela vient du fait que, géographiquement, le pays est moins touché par les migrations en lien avec la crise syrienne que ceux d'Europe du Sud-Est et de l'Est. Cette priorisation ne résulte pas d'un document officiel mais des perceptions constatées en lien avec les discours publics.

Les questions migratoires font l'objet d'une attention particulière, et sont pour le moment mises en avant plus particulièrement par l'**Italie** et le **Portugal** dans les différents rapports. L'**Italie** est, avec la Grèce, le pays de l'Union européenne (UE) le plus touché par les flux migratoires en provenance de pays tiers, et identifie la migration comme une menace pour sa sécurité. Il en va de même pour le **Portugal**, ce qui tend à démontrer que les pays du Sud sont plus concernés par ces problématiques que les pays du Nord de l'Europe. La migration ne constitue bien évidemment pas en soi une menace de sécurité, comme le souligne le rapport italien. En revanche, l'arrivée massive de migrants telle qu'on la vit aujourd'hui empêche une gestion efficiente des frontières européennes. Ainsi, le flux migratoire constitue un facilitateur pour la circulation de criminels qui profitent des dysfonctionnements de contrôles pour entrer sur le territoire européen malgré l'utilisation croissante de dispositifs de plus en plus performants, notamment les technologies biométriques dont les gardes-frontières font utilisation dans les centres d'hébergement grecs et italiens. En outre, le nombre important de réfugiés crée des instabilités politiques et sociales au sein des États dans lesquels la population est hostile à les accueillir, animant les tensions entre les communautés et desservant leur intégration, soit-elle temporaire. Le rapport portugais insiste notamment sur la nécessité d'établir un consensus politique sur les implications sociétales du phénomène au sein des États avant de mettre en place quelque politique que ce soit. Or, on constate que ce consensus, difficile à trouver au niveau national, l'est encore plus au niveau européen, le discours de la chancelière allemande sur le nécessaire accueil des réfugiés étant loin d'être partagé par tous, notamment en Europe de Nord ou dans certains pays d'Europe de l'Est.

Les pays du Sud et de l'Est sont dans les faits les principaux touchés par l'ampleur des flux migratoires. La relocalisation et la réinstallation de migrants au sein d'autres États membres que ceux par lesquels ils sont entrés dans l'espace Schengen a pour but de répartir le fardeau de la gestion des frontières extérieures, laissées à la compétence des autorités nationales, dans toute l'Europe. Bien que cette mesure n'ait aujourd'hui que très partiellement été mise en œuvre, elle illustre parfaitement un phénomène d'*européanisation de la menace et des risques*, tant dépendant des facteurs énoncés précédemment – évolution technologique et mondialisation – que de l'intégration de la gestion des problématiques de sécurité dans l'Union européenne.

Aux **Pays-Bas**, les priorités diffèrent. La lutte contre le terrorisme et l'extrémisme constitue une menace importante, mais moins urgente que la manipulation de l'administration publique, la rupture d'approvisionnement en minerais et le cyber-espionnage[2].

En **France**, le Livre blanc sur la défense et la sécurité nationale de 2013 identifie comme priorités stratégiques les moyens devant être mis en œuvre pour assurer la protection des intérêts fondamentaux de la Nation, c'est à dire les agressions contre le territoire national, les attaques terroristes, les cyber-attaques, les atteintes au potentiel scientifique et technique, la criminalité organisée, les crises majeures d'origines naturelles ou humaines et les attaques contre les ressortissants à l'étranger. Ces menaces sont énumérées dans les documents stratégiques français, sans être véritablement priorisées. Mais, depuis les attentats de janvier puis de novembre 2015, le terrorisme est devenu la première des priorités alors que le phénomène migratoire se traduit par des tensions ponctuelles et réelles concentrées géographiquement sur certains points : Calais, Vintimille à la frontière franco-italienne et Paris dans une moindre mesure. Si la menace cyber est moins mise en avant, c'est avant tout parce que la France a réagi, notamment depuis la publication du Livre blanc sur la défense et la sécurité nationale de 2013, avec la publication d'une Stratégie nationale pour la sécurité du numérique en octobre 2015, et alors que la Défense a créé un poste d'officier général de cyber défense.

D'autres menaces existantes ou proches sont énumérées dans les rapports **néerlandais, italien, anglais et espagnol** et incluent la radicalisation, le conservatisme religieux, l'intégration des communautés musulmanes, les inégalités de richesses à l'échelle internationale et la corruption.

En conclusion, si l'on constate une certaine harmonisation de la perception des menaces au niveau européen en mettant globalement en avant le triptyque terrorisme, migration, cyber sécurité, cela ne doit pas cacher des différences dans le traitement même de la réponse apportée.

[2] According to the National Coordinator for Security and Counterterrorism, attached to the Dutch Ministry of Security and Justice which recently published a National Risk Assessment as part of the National Security Strategy.

Concernant le terrorisme, la perception de la menace est clairement plus forte au Sud qu'au Nord de l'Europe. Si la menace cyber est globalement mise en lien avec une menace extérieure alors que les autres pays mettront tout autant en avant l'origine privée – avec la cyber criminalité – ou terroriste d'une telle menace. L'Allemagne se distingue à ce niveau en mettant en avant les risques d'atteintes aux libertés publiques et à la vie privée, et ce en osmose avec les préoccupations de sa société civile. La question migratoire, qui n'est pas une menace en soi mais qui peut venir en conforter certaines, nécessite en tout état de cause des réponses en matière de sécurité, et est sans doute la plus susceptible d'entrainer des désaccords, non pas sur la constatation du phénomène mais sur l'attitude à adopter face à celui-ci. Cela entraine des divergences dans les réponses apportées, qui se traduisent par la difficulté de l'Union européenne à imposer les mesures qu'elle préconise. La question est dans ce cas bien posée à l'échelle de l'UE, mais les réponses ne sont apportées que très imparfaitement.

Face à ce constat, la nouvelle présidence néerlandaise du Conseil de l'Union a toutefois essayé, dès son entrée en fonction au premier semestre 2016, de déterminer un agenda commun en mettant en avant l'importance de la lutte contre le terrorisme et la cyber-sécurité – qui sont donc deux des menaces les plus communément citées par les Etats et ne font pas l'objet de divergences majeures entre eux – pour ces prochains mois. Ces priorités ne sont pas exclusives à l'orientation stratégique des institutions européennes, et les États préservent une marge de manœuvre tant sur leur définition que sur les moyens de combattre les menaces sécuritaires.

DE QUELLE MANIÈRE LES TECHNOLOGIES PEUVENT-ELLES CONSTITUER UNE RÉPONSE AUX MENACES SÉCURITAIRES ?

Les technologies de sécurité sont conçues, produites et commercialisées pour répondre aux menaces et aux risques existants ou, d'un point de vue prospectif, pressentis. Or, en résolvant un problème, la technologie de sécurité en crée parfois de nouveaux. Pour tous, les technologies de l'information et de la communication présentent une caractéristique : elles sont susceptibles de générer aussi bien des avantages que des d'inconvénients. En effet, les progrès technologiques s'accompagnent de nouveaux risques bien souvent liés entre eux. Les auteurs des différents rapports s'accordent sur les implications qui découlent de ces progrès.

Tout d'abord, l'*universalisation d'internet*. L'accessibilité et la démocratisation d'internet sont des objectifs poursuivis par les États européens, avec pour objectifs : de permettre aux individus d'exploiter le potentiel du web en terme de commercialisation et d'acquisition de biens et de services ; d'offrir aux entreprises et aux gouvernements une utilisation effective des outils numériques ; et de garantir aux sociétés du numériques et aux start-up un horizon aussi large que possible pour développer leurs activités. Or, comme le précisent les rapports **néerlandais, italien et portugais**, en facilitant à tous un accès aux réseaux, on facilite inévitablement l'accès à des personnes malintentionnées dont les compétences dans le domaine numérique peuvent engendrer des risques au degré de gravité variable. L'une des meilleures illustrations est celle du vol d'identité et de données bancaires. L'utilisation massive d'internet à des fins commerciales, couplée à l'insouciance des utilisateurs communicants naïvement leurs données personnelles, offrent aux usurpateurs un potentiel démesuré pour la réalisation de leurs intentions délictuelles ou criminelles.

Pour **l'Espagne,** l'évolution et l'innovation technologies créent de nouvelles menaces inconnues jusqu'alors. Les progrès dans le domaine de la chimie, du nucléaire, du biogénétique, ainsi que dans le domaine numérique sont incontournables, pourtant ils créent de nouveaux enjeux pour l'intégrité, la prospérité et le bien-être des sociétés, ainsi que pour la protection de leur peuple et de leur propriété.

En **Pologne**, les systèmes de surveillance et les softwares pour détecter les cyber-attaques sont listés parmi les technologies les plus prometteuses.

Un autre phénomène est celui de *l'accumulation et du stockage de données*. Il s'agit d'un outil indispensable pour les services de renseignement à des fins de prévention et de détection d'infractions pénales, ou simplement sur la base de stockage de données à partir du profilage des utilisateurs d'ordinateurs. Si l'utilisation de données numérisées permet d'accroitre les capacités et l'effectivité des autorités en charge de la sécurité

publique, elle peut tout autant porter atteinte aux libertés et droit fondamentaux des individus concernés par un traitement abusif de ces données. La notion de traitement abusif est une notion soumise à interprétation, notamment du juge en cas de contentieux. Elle s'apprécie en revanche selon des critères fixes qui reposent sur les principes de proportionnalité et de nécessité. Le traitement de données à caractère personnel doit répondre à une finalité déterminée, et les moyens utilisés doivent se limiter au minimum pour atteindre cette finalité. Il est important de faire une interprétation stricte de ces critères en vue de garantir la meilleure protection des droits fondamentaux et des libertés individuelles de protection des données à caractère personnel et de respect de la vie privée, auxquels il n'est possible de porter atteinte que dans des hypothèses très limitées, réservées aux atteintes graves et imminentes à l'ordre public, comme le prévoit par exemple la Constitution **allemande**.

Outre les atteintes qu'il est susceptible d'engendrer quant au respect des droits individuels, le stockage massif de données sensibles, notamment celles détenues par les autorités publiques, constitue une cible pour le cyber-espionnage d'État à État.

Les *objets connectés* ou l'internet des objets sont également un produit de l'innovation technologique dont les implications sont de deux ordres. L'**Italie** expose que, dans une perspective d'accroissement du confort individuel, ils sont très appréciés et prolifèrent, occupant une place de plus en plus importante dans le quotidien de chacun. Séduits par le potentiel d'optimisation de gestion du temps ou d'organisation, les individus, les entreprises, les administrations publiques emploient de plus en plus d'objets connectés pour effectuer des tâches courantes. Pourtant, la cyber-résilience de ces appareils n'est pas optimale. Les risques peuvent tout autant dépendre d'une défaillance technique que d'une intrusion malveillante dans les systèmes. La vulnérabilité de ces objets crée par ricochet une vulnérabilité des objets auxquels ils sont connectés, multipliant d'autant les facteurs de risques. Le rapport **britannique** met même en évidence le risque futur que pourraient présenter des objets qui se comporteraient de plus en plus comme des automates et qui échapperaient à tout contrôle humain.

Pour tous, les *médias sociaux* sont aujourd'hui l'une des meilleures plateformes collaboratives de communication et de partage d'informations. Ils offrent aux utilisateurs un accès continu et instantané à l'information, qu'ils communiquent et partagent eux-mêmes. Malheureusement, l'utilisation massive de cet outil empêche un contrôle efficient des propos pouvant être tenus, de leur véracité et de leur caractère haineux ou discriminant. Ainsi, ils sont dans un même temps l'outil le plus efficace pour la propagande et, en matière de terrorisme, de recrutement et de radicalisation, comme le souligne le rapport britannique.

Pour autant, les progrès technologiques en matière de sécurité sont autant une réponse qu'une menace potentielle dans une sorte de dialectique empruntée à la défense qui mettrait en perpétuelle confrontation l'épée et le bouclier.

On peut ainsi citer les recherches faites en matière d'informatique quantique qui, outre la démultiplication de la vitesse des ordinateurs, devrait permettre d'identifier les attaques cyber.

Le rapport **italien** note qu'il existe une forme de *monopole du secteur privé sur l'orientation de la recherche dans le domaine des technologies de l'information et de communication*. Dans le domaine de la recherche, on remarque que ces technologies sont en effet au cœur de nombreux programmes au sein des entreprises. L'innovation profite à tous les acteurs de la sécurité, publics comme privés mais également, au sein de la sécurité publique, des forces de police comme des forces militaires. La dualité de ces technologies, c'est à dire le fait qu'elles puissent avoir des applications tant civiles que militaires, est bénéfique en termes de synergie et de mutualisation des ressources destinées à la recherche. Toutefois, dans le domaine des technologies de l'information et de la communication, le secteur civil occupe une place de plus en plus importante par rapport au secteur public. Ainsi, bien que ces nouvelles technologies soient étroitement liées à la sécurité, et notamment la cyber-sécurité, les autorités justement en charge d'assurer la sécurité publique sont dépendantes des choix des opérateurs civils en matière d'orientation de la recherche et de l'innovation.

L'**Espagne** met en avant les nouvelles technologies qui ont été mis en service et qui apportent des progrès en matière de sécurité. Sont cités le système intégré de surveillance des frontières utilisé pour la reconnaissance des navires, les systèmes de simulation des forces de sécurité et les technologies utilisées pour la reconnaissance des explosifs utilisées dans les IED (*improvised explosive device*).

Tous les rapports mettent en évidence les progrès enregistrés en matière de technologies de l'information, qui permettent de recueillir des données sur les individus par le biais de leur téléphone et de leurs ordinateurs ou de développer les capacités de lutte contre un certain nombre de criminalités, à commencer par le terrorisme qui figure en tête des préoccupations. Mais ces technologies, qui sont destinées à accroitre la sécurité, sont également porteuses de deux menaces potentielles : la vulnérabilité croissante aux attaques cyber et l'atteinte aux libertés publiques. Ainsi, le rapport britannique met en avant le fait que la possibilité de développer un ordinateur quantique permettrait d'avoir accès à toute information cryptée, ce qui constituerait aussi bien un progrès qu'une menace contre les intérêts des États.

Mises à part les technologies de l'information et de communication mentionnées dans les différents rapports, d'autres technologies sont au cœur des préoccupations. Ainsi, pour l'**Italie**, l'attention doit être portée sur les logiciels de surveillance, sur les micro-caméras et la reconnaissance faciale, ainsi que sur les drones. Pour l'**Allemagne**, il convient de surveiller l'évolution des technologies pour la rétention de métadonnées, les logiciels de cryptage de communications électroniques et la collecte des données de mobiles. Pour les **Néerlandais**, les enjeux résident dans les technologies biométriques, d'authentification et d'identification, et celles utilisées pour l'analyse comportementale.

D'autres débats, actuels et futurs, portent sur la robotisation de la sécurité, comme l'évoque le rapport **néerlandais**. Les drones et les robots armés sont les principaux systèmes concernés. Les drones, mis à part les enjeux qui en découlent en termes de protection de la vie privée liés à leur fonction de surveillance, se révèlent également dangereux pour la sécurité physique et aérienne, plus précisément en cas de défaillance technique ou de détournement. Les robots, quant à eux, peuvent soulever les débats publics sur la déshumanisation de la sécurité ou de la guerre dans le domaine de la défense.

QUELLES SERAIENT LES DISPOSITIONS LÉGISLATIVES SUSCEPTIBLES D'APPORTER DES RÉPONSES ?

Tous les États concernés par l'étude disposent de stratégies de sécurité portant sur des aspects particuliers, comme celles pouvant avoir trait aux politiques cyber. On peut préciser qu'il en est de même pour l'Union européenne qui dispose, depuis 2003, d'une stratégie de sécurité européenne relative à la sécurité extérieure de l'Union. Sa définition et sa mise en œuvre relèvent du Service européen pour l'action extérieure et, depuis 2010, d'une stratégie de sécurité intérieure. Les stratégies de sécurité l'Union étant antérieures à celles de ses États membres, elles ont eu un impact sur les approches nationales puisque celles-ci se sont appuyées sur l'existant. Le processus législatif pour la mise en œuvre des stratégies se traduit par l'adoption de lois plus spécifiques pour atteindre les objectifs que les stratégies poursuivent.

Les États concernés par l'étude s'intéressent en priorité à trois sujets : le cyber, le terrorisme et la gestion migratoire, ce qui n'est pas surprenant car ces trois sujets font partie des priorités en termes de sécurité.

Dans le domaine du cyber, les législations sont quasi-inexistantes ou très récentes. En **France**, un projet de loi sur le numérique est en cours d'élaboration début 2016. Il ne s'agit pas seulement de la première loi sur le sujet, mais également du premier texte pour lequel les citoyens ont pu contribuer à la rédaction, en proposant des amendements *via* une consultation publique en ligne, selon une logique de démocratie directe.

Les autres pays européens n'indiquent pas disposer de lois d'application, mais ils disposent de stratégies sur ce sujet, comme l'État français et l'Union européenne. Comme le précise le rapport **néerlandais**, pendant plus de dix ans, le seul texte en matière de cyberespace était la convention de Budapest de 2001 contre le cyber-crime. Cet accord international n'a pourtant pas été ratifié par le plus grand nombre et n'a, jusqu'à présent, pas démontré sa réelle efficacité. Pour pallier le vide dans le domaine cyber, la majorité des pays de l'étude s'est dotée dès 2013 d'un document stratégique sur le sujet, ainsi que de structures dédiées à la gestion de ces problématiques. La **France** et l'**Allemagne** se démarquent des autres pays puisqu'ils ont débuté les travaux publics sur les enjeux du cyberespace dès 2011, c'est à dire deux ans avant leurs partenaires.

En **Allemagne**, l'adoption de la stratégie de cyber-sécurité s'est accompagnée de la création de plusieurs nouveaux organismes en charge de son application. Dans le domaine militaire, Berlin dispose depuis 2002 d'un *Computer Emergency Response Team* (CERTBw). Pour le domaine de la sécurité cybernétique non militaire, un Conseil national de cyber-sécurité a été créé en 2011, après qu'ait été publiée la Stratégie de sécurité cyber, qui sert de plate-forme aux utilisateurs pour échanger leurs expériences

et leurs stratégies. Un *National Cyber Response Centre* a été également crée en 2011, qui sert de plate-forme collaborative pour les agences gouvernementales comme l'Office fédéral pour la sécurité de l'information, la police et les agences de renseignement.

En **Espagne**, la stratégie de cyber-sécurité a été adoptée en 2013, conformément aux ambitions de la Stratégie nationale de sécurité de 2012. La gouvernance s'effectue, pour les affaires intérieures, au sein du *National Police and Civil Guard* en charge de la sécurité des infrastructures critiques ainsi que de la lutte contre le cyber-crime et le cyber-terrorisme. Le ministère de l'Industrie a développé sa culture de cyber sécurité via l'Institut national de cyber sécurité (INCIBE en Espagne). Le ministère de la Défense s'est quant à lui doté d'un *Joint Cyber Defense Command* et d'un Centre national pour le renseignement (CNI), respectivement pour la conduite des opérations de cyberdéfense et la protection des systèmes d'information et de communication des administrations publiques.

L'**Italie** a adopté en 2014 un cadre de travail national pour la sécurité et la protection du cyberespace. Les documents stratégiques établissent l'architecture institutionnelle et identifient les administrations en charge de la mise en œuvre des politiques nationales de cyber-sécurité. Parmi celles-ci, le Comité interministériel pour la sécurité de la République propose les nouvelles mesures législatives, l'Unité de cyber sécurité destinée à répondre aux incidents cybers, et le *Security Intelligence Department* qui joue entre autre le rôle de coordinateur au niveau national.

L'Union européenne s'est elle-même dotée en 2013, d'une stratégie européenne de cyber sécurité. Bien que celle-ci n'ait pas une valeur juridique contraignante, on remarque qu'elle a pu avoir un impact sur les politiques nationales, puisque c'est suite à sa publication que les États ont adopté des mesures en propre.

Pour l'instant, les législations nationales **dans le domaine numérique** ont pour objet les questions suivantes : le traitement de données à caractère personnel et les engagements de l'organisme responsable de leur traitement ; le pouvoir des autorités judiciaires et de police ; et la protection des droits et libertés des citoyens.

En **France**, la loi de 1978 devrait être modifiée.

En **Allemagne**, le Parlement a adopté en octobre 2015 une loi sur la conservation et le traitement des données, obligeant les opérateurs de télécommunications et les fournisseurs d'accès internet à fournir les données relatives à l'utilisateur du téléphone, la personne appelée, la date de l'appel, sa localisation, et dans le cas d'internet l'adresse IP ainsi que la date de la connexion. Cette loi s'applique en cas de présomption d'un crime sévère, tel que prévu par la Constitution (§ 100g StPO). Les données seront traitées par l'Agence fédérale des réseaux de télécommunications et d'internet.

Au niveau de **l'Union européenne**, le paquet européen sur la protection des données devrait être formellement adopté en avril 2016, après quelques quatre ans de débat. Ce

paquet se compose d'un règlement relatif au traitement des données par les opérateurs économiques et d'une directive sur le traitement des données par les autorités policières et judiciaires. D'ici deux ans, sauf disposition contraire, les États devront avoir adapté leur législation nationale au contenu de ces deux textes.

On remarque que ces propositions sont davantage destinées à garantir la sécurité individuelle dans le cadre d'activités cyber plutôt que la cyber-sécurité à proprement parler. Il faudra attendre l'adoption officielle de la directive européenne sur le niveau minimum de sécurité des réseaux d'information, qui devrait intervenir en 2016, pour que les États légifèrent en matière de cyber sécurité *per se*. Cela veut dire que ces États disposeront au plus tard d'une législation d'ici deux ans, période donnée pour pouvoir transposer une directive en droit interne. Les États ne souhaiteront donc pas légiférer sur le sujet avant cette date, puisque leurs législations devront être conformes à cette directive.

Dans le domaine de la lutte contre le terrorisme, tous les États ont adopté des législations nationales relatives à la lutte et l'incrimination du terrorisme. Ces lois condamnent la propagande, l'entrainement, la préparation d'attentats et leur financement. Ces activités sont qualifiées d'acte criminel. La définition de l'infraction terroriste repose sur deux catégories d'éléments. L'action doit comporter des éléments objectifs – par exemple un homicide –, des préjudices corporels ou une prise d'otage. L'action doit également comprendre des éléments subjectifs, tels que l'intimidation de la population ou la déstabilisation du pays. Cette décision reconnaît également la condamnation de l'intention, des actes préparatoires, d'une infraction en lien avec des activités terroristes. En d'autres termes, cette décision n'exige pas que l'infraction ait été consommée pour être condamnée. L'appréciation de l'intention repose sur une interprétation subjective.

L'**Italie** a également adopté une loi, en avril 2015, qui étend le cadre légal pour la surveillance opérée par les autorités de renseignement dans le cadre de leur lutte contre le terrorisme

Au **Royaume-Uni**, David Cameron a proposé en juillet 2015 une loi sur les pouvoirs d'investigation, l'*Investigatory Powers Bill,* qui oblige les entreprises à conserver les enregistrements pour une durée minimum d'un an, afin de pouvoir les mettre à disposition des forces de sécurité si nécessaire. Le projet de loi prévoit également la possibilité de bénéficier de la part des opérateurs de *backdoor access* afin d'avoir accès à des informations cryptées.

Même la **Pologne** prépare sa première loi anti-terroriste – *Ustawa antyterrorystyczna* – dans la foulée des attentats en France de novembre 2015. Celle-ci doit prévoir un cadre légal pour les activités contre-terroriste qui sont identifiées dans le Programme national de lutte contre le terrorisme (2015-2019). On peut interpréter cela comme le fait que la lutte contre le terrorisme devient progressivement une priorité pour ce pays, jusqu'à

présent en retrait sur le sujet. Les consultations sur cette nouvelle loi doivent se poursuivre au printemps 2016.

En **Espagne**, la loi organique sur la protection de la sécurité publique, qui remplace la loi organique du 1/1992 sur le même sujet, a été adoptée le 30 mars 2015. Cette loi prévoit un certain nombre de dispositions qui sont considérées plus restrictives que celles existant antérieurement en matière de liberté publique. Ainsi, l'appel à protester *via* les réseaux sociaux pourra être pénalisé, ainsi que le fait de prendre en photos des policiers ou de s'opposer à une expulsion.

Frappée par deux séries d'attentats en janvier et novembre 2015, la **France** a par ailleurs proposé dès l'été 2015 plusieurs projets législatifs pour lutter contre le terrorisme, notamment avec une loi sur le renseignement. Celle-ci, adoptée en juillet 2015, a certes permis d'encadrer les activités des autorités de renseignement ce qui n'était pas le cas auparavant,––, mais elle a également permis de légaliser des pratiques pouvant être considérées comme portant atteinte aux droits de l'Homme, notamment concernant les techniques utilisées pour collecter le renseignement. La loi prévoit de pouvoir contraindre les fournisseurs d'accès à Internet à détecter une menace terroriste sur la base d'un traitement automatisé et en surveillant tout le trafic. Des boîtes noires sont chargées d'examiner les métadonnées de toutes les communications : origine ou destinataire d'un message, adresse IP d'un site visité, durée de la conversation ou de la connexion, etc. Le Conseil constitutionnel a toutefois validé l'essentiel de cette loi, soulignant que « la décision de recourir à des techniques de recueil de renseignement et le choix de ces techniques devront être proportionnés à la finalité poursuivie et aux motifs invoqués. Il en résulte que les atteintes au droit au respect de la vie privée doivent être proportionnées à l'objectif poursuivi. La Commission nationale de contrôle des techniques de renseignement et le Conseil d'État sont chargés de s'assurer du respect de cette exigence de proportionnalité[3] ».

Politiquement et juridiquement, cette décision est importante car elle ne remet pas en cause le principe de la collecte d'informations privées pour lutter contre le terrorisme. En revanche, elle fixe aux autorités publiques des limites en terme de proportionnalité des démarches intrusives en matière de renseignement, et ce au regard du risque encouru. Le débat devrait donc normalement se déplacer sur le terrain de l'organisme chargé du contrôle, ainsi que les techniques éventuelles d'autoprotection des données privées, avec le concept du *privacy by design*.

Au niveau de **l'Union européenne**, le paquet européen sur la protection des données devrait être formellement adopté en avril 2016. Comme évoqué précédemment, ce paquet se compose d'un règlement relatif au traitement des données par les opérateurs économiques et d'une directive sur le traitement des données par les autorités policières

[3] Conseil constitutionnel, Décision n° 2015-713 DC du 23 juillet 2015 - Loi relative au renseignement, Communiqué de presse, 23 juillet 2015.

et judiciaires. La directive concerne la protection des individus face au traitement de leurs données à caractère personnel dans le cadre d'activités de police ou judiciaires, tandis que le règlement s'attache à encadrer le traitement de données par les opérateurs économiques – les entreprises. Les cadres de traitement, applicables aux opérateurs privés ou publics, sont en fait étroitement liés. Les entreprises établies sur le territoire de l'Union transfèrent régulièrement, dans le cadre de leurs activités commerciales ou de ressources humaines, des données vers des entreprises américaines. Cette pratique se faisait dans le cadre légal de la décision *Safe Harbor* (accord entre l'UE et les USA pour le transfert de données), récemment invalidée par la cour de justice de l'Union européenne au motif que les citoyens de l'Union ne pouvaient voir leur droit à la vie privée et à la protection des données à caractère personnel garanti par les autorités américaines, et qu'il leur était impossible de bénéficier d'un recours effectif devant les juridictions américaines[4]. Les autorités policières américaines peuvent en effet, grâce au *Patriot Act* de 2001, accéder aux données détenues par les opérateurs privés américains dans le cadre de leur mission de sécurité, et notamment de lutte contre le terrorisme. L'adoption, informelle à ce jour, du paquet européen sur la protection des données, couplée à l'invalidation du *Safe Harbor* offre aux citoyens de l'UE les garanties jugées nécessaires par les pouvoirs publics communautaires. Là encore, on peut noter que ces propositions sont davantage destinées à garantir la sécurité individuelle dans le cadre d'activités cyber plutôt que la cyber-sécurité à proprement parler. Le paquet « protection des données » devrait être officiellement adopté au printemps 2016, tandis que le *Safe Harbor* vient d'être remplacé par le *Privacy Shield*, qui propose des garanties plus claires et des obligations de transparence concernant le rôle du gouvernement des États-Unis. Si la directive et le règlement européens sont adoptés en 2016, les États devront adapter leur législation nationale au contenu de ces deux textes, ce qui pourrait se traduire par une remise en cause de certaines législations déjà adoptées.

Parallèlement à l'adoption de nouvelles lois, la **France** a proposé de réviser sa Constitution afin d'y introduire le principe de déchéance de nationalité pour les auteurs d'actes terroristes. Toutefois, il n'est pas certain que cette révision constitutionnelle, qui nécessite une majorité des trois cinquièmes du Parlement réuni en Congrès, soit adoptée. Certains ne souhaitent pas que cette mesure figure dans la Constitution. De plus, limiter cette mesure aux binationaux risquerait de conduire à une rupture de l'égalité devant la loi, alors que l'étendre à tous pourrait être contraire à la convention de New York de 1954 destinée à lutter contre les apatrides.

La gestion migratoire est une prérogative régalienne, bien que la création de l'espace Schengen conduise à relativiser son principe.

L'espace Schengen est un espace sans frontières intérieures, c'est-à-dire que seules les frontières extérieures de cet espace sont contrôlées. La libre circulation des biens, des personnes et des marchandises est y est garantie. Bien que la libre circulation soit un

[4] CJUE, 6 octobre 2015, Max Schrems, aff. C362/14, non encore publié au recueil.

principe fondamental, le « code frontières Schengen » permet aux États membres de rétablir temporairement les contrôles frontaliers pour des raisons d'ordre public et de sécurité (art. 23 et suivants). Or, les mesures de contrôle aux frontières se sont multipliées depuis 2015 pour la première fois depuis la mise en place de Schengen.

C'est sur cette base juridique que la **France** a rétabli le contrôle à ses frontières entre le 13 novembre, suite aux attentats qui ont frappé sa capitale et pour s'assurer du bon déroulement de la COP21. Les autres cas de contrôle aux frontières qui se sont multipliés depuis septembre 2015 ont pour objet de permettre aux États de maîtriser les flux de migrants. C'est notamment le cas de la Suède, du Danemark, de l'Autriche, de la Hongrie, de la République tchèque, de la Slovénie, de l'Italie et de la Belgique. L'Allemagne concentre à elle seule une grande part de cette problématique, puisqu'après avoir annoncé sa volonté d'accueillir les migrants, elle a dû prendre des mesures correctives sous forme de contrôle aux frontières pour faire face à des flux massifs et incontrôlés.

Un certain nombre de lois sont adoptés dans les pays européens, ayant pour objet de dissuader les migrants et de contribuer à la prise en charge dans leur pays d'accueil. La loi danoise votée à la fin du mois de janvier 2016 prévoit la confiscation des biens des migrants au-delà d'un seuil de 1340 euros. En Allemagne, un certain nombre de Lander pratiquent également une telle politique pour les demandeurs d'asile. C'est le cas de la Bavière et du Bade-Wurtenberg, le seuil de confiscation étant respectivement de 750 euros et 350 euros.

En France, l'état d'urgence – qui permet notamment de procéder à des perquisitions administratives, à des fouilles des véhicules et à des assignations à résidence – a été décrété pour 3 mois suite aux attentats du 13 novembre 2015, puis prolongé pour 3 mois supplémentaires. La mesure doit être inscrite dans la réforme de la Constitution étudiée au début de l'année 2016. Par ailleurs, la réforme du Code de procédure pénale prévoit la mise en place d'autres mesures, comme des retenues administratives de quatre heures lors de contrôles d'identité, la fouille de véhicules à proximité des lieux sensibles ou l'assignation à résidence pour les individus suspectés de revenir de Syrie.

Le **Royaume-Uni** n'est pas membre de l'espace Schengen. Il n'en demeure pas moins que ce pays soit très préoccupé par les problématiques migratoires. L'accès très contrôlé au territoire britannique crée des répercussions sur le sol français, où de nombreux migrants séjournent dans des conditions précaires sur la côte d'opale, espérant pouvoir atteindre le territoire britannique.

L'européanisation des risques migratoires a nécessité de repenser les modes de gestion. En 2004, **l'Union européenne** s'est dotée d'une Agence pour la gestion de ses frontières extérieures – l'agence Frontex – dont le rôle consiste essentiellement à coordonner et soutenir l'action des États membres. La plus-value de cette agence est remise en question depuis le début de la crise migratoire. Les ressources propres aux États périphériques en charge du contrôle des frontières extérieures ne suffisent pas, et bien que Frontex dispose, depuis 2004, de la capacité d'acquérir du matériel additionnel, cela

n'a pas été suffisant pour doter les États concernés des équipements nécessaires. De plus, malgré les nombreux appels aux dons lancés par Frontex auprès des États membres, peu ont été enclins à fournir du matériel à titre gracieux.

Ceci étant, avec l'adoption de mesures provisoires successives, l'Union européenne a essayé de prendre des initiatives en complément à l'action des États membres, décidant d'opérer des actions immédiates pour faire face à une crise sans précédent, parmi lesquelles la relocalisation et la réinstallation des réfugiés ou de ceux prétendant au statut de réfugié et la mise en place de « hotspots ». Cette dernière mesure, appliquée aux lieux les plus touchés par l'arrivée massive de migrants – Grèce et Italie – se destinait à désengorger les flux tout en garantissant un contrôle effectif des personnes entrant sur le territoire de l'Union. L'installation de ces hotspots est longue et fastidieuse, et leur efficacité ne peut être appréciée à ce jour. Parallèlement, et consciente que des actions immédiates et des mesures provisoires ne suffiront pas à résoudre les problématiques migratoires, l'Union européenne a proposé en décembre 2015 un « paquet frontières ». Ce paquet inclut : une proposition de règlement pour la création d'une nouvelle agence européenne de gardes-frontières et de garde-côtes européens, qui remplacerait l'actuelle agence Frontex ; une révision du code frontières Schengen ; et une proposition de règlement sur un document de voyage européen pour les tiers séjournant de manière illégale sur le territoire de l'UE. Ce document de voyage illustre accessoirement l'utilisation croissante des données biométriques pour améliorer l'effectivité du contrôle des flux migratoires en Europe. L'adoption du « paquet frontières » est attendue à l'issue du premier semestre 2016.

De nouvelles structures dédiées à la sécurité

En France, l'Agence nationale de sécurité des systèmes d'information (ANSSI) a été créée en 2009, remplaçant la Direction centrale des systèmes d'information. Elle assume le rôle d'autorité nationale en matière de sécurité des systèmes d'information. Plus récemment, en 2013, le Conseil des industries de confiance et de sécurité (CICS) et le Comité de filière des industries de sécurité (Cofis) ont été mis en place pour renforcer le dialogue entre les pouvoirs publics et les industriels de la sécurité, la connaissance de la demande publique dans le secteur étant essentielle à l'efficience de la mise en œuvre des politiques publiques de sécurité.

Au niveau de la formation, la création d'un campus de la sécurité intérieure à Lyon a été proposée en 2013. Cette proposition s'inscrit dans la continuité logique des implications de la ville dans le domaine de la sécurité. Lyon est un acteur international de la sécurité, particulièrement actif et important. La ville accueille aujourd'hui le siège d'Interpol, le siège de l'Institut national de la police scientifique, la sous-direction de la police technique et scientifique de la police judiciaire et le siège de l'École nationale supérieure de police. Le campus offrirait une plate-forme de partage pour les différentes écoles, académies, collèges européens, instituts et centres de recherche de police, dans le but de regrouper et d'harmoniser le développement des activités de sécurité intérieure et de

rapprocher les formations. Cette ambitieuse initiative, soutenue par le ministère français de l'Intérieur et Interpol, répond aux besoins de coordination pour lutter contre les nouvelles menaces sécuritaires et se destine à devenir un pôle d'excellence européen.

QUELS SONT LES DÉBATS PUBLICS, EXISTANTS OU FUTURS, POUVANT INFLUENCER LES MESURES DE LUTTE CONTRE LA MENACE SÉCURITAIRE ?

Les principaux débats publics résident dans l'opposition entre l'exercice des prérogatives de sécurité et des libertés individuelles, souvent résumée par l'expression *security vs. privacy*. Les différents rapports s'accordent pour mettre en évidence que les révélations d'Edward Snowden, portant essentiellement sur l'usage abusif des données relatives aux individus par les services de renseignement américains, ont conduit la société civile à se mobiliser contre les atteintes au respect de leur vie privée. Il en va de même concernant la protection des données à caractère personnel, les populations dénonçant les pratiques de forces de l'ordre jugées trop intrusives par rapport à l'objectif de sécurité poursuivi. Mais parallèlement, cette même société civile va accepter – voire demander – des réponses sécuritaires qui peuvent se traduire par la restriction des libertés publiques. Ce paradoxe est parfois inhérent aux progrès technologiques, et ce sans même que les autorités publiques ne prennent des dispositions restrictives.

La numérisation des sociétés crée en effet deux phénomènes corrélés. Tout d'abord, la possibilité pour les citoyens de bénéficier de services en ligne pour lesquels ils communiquent leurs données privées – telles que celles relatives à leur identité, leurs coordonnées bancaires, leur localisation géographique, mais aussi leurs centres d'intérêts –, permettant de reconstituer le profil des individus et d'anticiper leurs actions. Dans un même temps, la communication de toutes ces données permet aux forces de l'ordre d'exploiter une multitude de nouveaux canaux, ouvrant un champ nouveau pour poursuivre leurs investigations contre des criminels ou des terroristes.

Malgré tous les débats et toutes les polémiques sur l'usage abusif des données à caractère personnel par les autorités policières, force est de constater que la tendance selon laquelle les citoyens transmettent délibérément les informations les concernant ne régresse pas, bien au contraire. Ainsi, pour pouvoir bénéficier du confort de vie offert par les services numériques, les citoyens mettent eux-mêmes en péril la protection de leur vie privée et la protection de leurs données à caractère personnel.

Le rapport i**talien** insiste ainsi sur l'importance pour les autorités publiques de sensibiliser leurs ressortissants sur les vulnérabilités auxquels ils s'exposent du fait de l'usage de services numériques, même si le respect des droits et libertés fondamentales des citoyens est une obligation qui incombe aux États, indépendamment de ces comportements individuels. Les citoyens doivent donc pouvoir s'appuyer sur des garde-fous pour limiter les risques d'abus.

Ensuite, la question est de savoir qui du législateur ou du pouvoir judiciaire viendra arbitrer entre les préoccupations de sécurité et celles de liberté. En tout état de cause, le débat traverse tous les pays au sein de **l'Union européenne**, mais les réponses n'y sont pas identiques.

On constate en **Allemagne** que le pouvoir judiciaire est très présent dans le débat. Il est, comme ailleurs, le garant des libertés publiques, mais la question prend un relief tout particulier dans ce pays. Le rapport met en évidence ce rôle. La Cour constitutionnelle fédérale allemande a, par exemple, jugé en 2008 que la lecture automatique des plaques d'immatriculation violait le droit à la vie privée car elle ne répondait pas à une finalité déterminée, critiquant le principe de surveillance de masse. Plus près de nous, la loi sur la conservation des données des personnes ayant commis un crime sévère, votée par le Bundestag en octobre 2015, a été déférée à son tour devant la Cour constitutionnelle allemande.

Si le juge peut limiter les risques, le législateur lui peut les créer. En **Italie**, un décret sur la lutte anti-terroriste a été amendé pour permettre aux autorités publiques d'accéder aux ordinateurs personnels, soulevant de vifs débats dans la société civile. Cet amendement a finalement été supprimé par Matteo Renzi en avril 2015.

Au **Royaume-Uni**, le débat sur l'*Investigatory Powers Bill* – surnommé par ses opposants le *Snoopers' charter*, la charte des espions – n'a pas cessé depuis que le projet de loi a été déposé. Celui-ci est perçu de manière négative par la société civile, qui y voit une loi anti-Snowden tant elle étend les capacités d'accès aux communications téléphoniques et aux accès internet pour les autorités de police. Mais il est également rejeté par les opérateurs et fournisseurs de services numériques. Ceux-ci considèrent que l'*Investigatory Powers Bill* ne leur permettra plus de protéger les données privées de leurs clients. Apple a dénoncé notamment la possibilité pour les autorités publiques de bénéficier de *backdoor access* sur les données cryptées, ce qui pour cette firme fragilise de manière générale tous les dispositifs de protection des données. Les pétitions se multiplient au Royaume-Uni, sans que le projet de loi ait été sensiblement amendé pour le moment.

La nouvelle loi sur la sécurité en **Espagne** a également entrainé des protestations. Dans ce cas, la législation ne vise pas à étendre le recueil des données personnelles afin de lutter contre le terrorisme, mais plutôt à limiter les actions de revendications sur la voie publique – ce qui a conduit les opposants à parler de *gag law* (loi du bâillon). Elle vise donc plutôt les mouvements sociaux qui se sont faits jour suite à la crise économique en Espagne.

En **France**, la loi sur le renseignement a également provoqué de vifs débats par l'étendue des pouvoirs qu'elle donnait aux autorités policières en matière de collecte d'informations. Toutefois, ce débat ne semble pas avoir atteint l'intensité rencontrée au Royaume-Uni, même si la pétition « ni pigeons ni espions » a permis de fédérer plusieurs hébergeurs et fournisseurs d'accès internet, ainsi que le Conseil national du numérique. La Commission nationale informatique et libertés (CNIL) a elle-même donné un avis très réservé sur le sujet, notamment quant à l'utilisation des données et les durées de conservation de celles-ci.

La protection de la vie privée est assujettie à l'évolution de l'environnement sécuritaire. Plus un pays est vulnérable ou se sent menacé, plus il risque de légiférer au détriment des libertés individuelles. Les atteintes à ces libertés sont, dans cette hypothèse, légitimées par la menace et le besoin de disposer des moyens nécessaires pour y faire face. De cette manière, les gouvernements espèrent obtenir le soutien de leurs ressortissants. Sur ce sujet, les médias jouent également un rôle très important. Ils disposent d'un pouvoir d'influence sérieux et peuvent, par ce biais, sensibiliser les citoyens sur les risques liés à l'utilisation d'internet ou légitimer de nouvelles législations édictées pour des préoccupations de sécurité.

Le rapport **italien** précise que la sensibilisation aux problématiques de sécurité n'est pas équivalente dans toute l'Europe. L'Europe de l'Ouest, la **France, le Royaume-Uni et les Pays-Bas** sont les pays où les citoyens sont le plus sensibilisés à ces questions. En revanche, les pays du Sud se préoccupent davantage des problématiques migratoires, tandis que les pays de l'Est s'impliquent en priorité sur la protection et l'intégrité de leur territoire.

La manière dont les États légifèrent en matière de protection des données varie au sein de l'Union européenne, et trahissent des perceptions différentes sur la protection qui doit être assurée à l'individu contre les intrusions dans sa la vie privée, que celle-ci proviennent des autorités étatiques ou d'entités privées. Au Sud ou à l'Est, les enjeux relatifs à la protection des données à caractère personnel paraissent alors plus accessoires, sans être pour autant ignorés.

Pour la protection des données à caractère personnel, qui est corrélée à l'exercice des activités de police et de renseignement, les États européens disposent également de structures dédiées.

L'**Italie** a par exemple, depuis 1996, une autorité de protection des données dont le rôle est de conseiller les pouvoirs publics et de veiller au respect du droit à la protection des données et à la vie privée dans l'élaboration des nouvelles législations pour l'exercice des activités répressives.

En **Allemagne**, au niveau fédéral et pour chacun des seize Lander, il existe un commissaire pour la protection des données à caractère personnel. Ils ont un rôle de contrôle du respect des règlementations pour le traitement de données auquel les opérateurs privés sont soumis. Ils ont également un rôle de médiateur.

Aux **Pays-Bas**, la mise en place d'une autorité de protection des données date également des années 1990, en droite ligne avec les recommandations de la directive européenne de 1995. Elle dispose d'un pouvoir d'enquête pour évaluer la conformité des traitements et des lois relatives aux traitements de données à caractère personnel vis-à-vis des libertés et droits fondamentaux.

En **Pologne** la *Data protection authority* (GIODO) a été créée en 1997. Il existe une obligation légale universelle visant à traiter les données à caractère personnel avectoute

l'attention requise. L'obligation de consigner les données à caractère personnel qui ont été collectées comprend un certain nombre d'exemptions, y compris pour celles qui sont classifiées et acquises au cours d'enquêtes préliminaires, et qui s'applique le plus part du temps aux entités commerciales. Le GIODO peut, à sa propre initiative ou après réception d'une plainte émanant d'une personne morale ou privée faisant état d'une utilisation abusive de ce type de donnée, lancer une procédure de contrôle. Le GIODO émet également un avis lorsqu'un nouveau texte législatif sur les données à caractère personnel est proposé.

En **Espagne**, la question de la protection des données personnelles est du ressort de l'Agence espagnole de protection des données personnelles – *Agencia Española de Protección de Datos*, AEPD –, qui est une agence indépendante. Celle-ci trouve ses origines dans la Constitution espagnole, dans la convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et de la directive 95/46/CE sur la protection des données personnelles des citoyens européens. Après la création de cette agence, le gouvernement a présenté en 2007 la loi sur la détention de données en lien avec les communications téléphoniques et numériques, qui a permis l'utilisation de banques de données par les services de sécurité sous le contrôle du pouvoir judiciaire. La législation espagnole semble donner satisfaction, puisque les plaintes pour violation des droits civils sont peu nombreuses. Les débats auxquels on assiste dans les médias sur la surveillance de masse dans le cadre des activités d'espionnage et de lutte anti-terroriste ne donnent pas lieu à des répercussions au plan national en Espagne.

Le précurseur en la matière reste **la France**, qui dispose d'une autorité depuis l'adoption de la loi de 78 dite informatique et libertés. La CNIL (Conseil national informatique et libertés) assure actuellement la présidence du groupe 29 (G29), qui est le groupement européen des autorités de protection des données européennes et qui œuvre à l'harmonisation des garanties de protection sur le territoire de l'Union.

L'Union européenne dispose par ailleurs d'une autorité de contrôle indépendante pour la protection des données, dont le rôle consiste à contrôler les traitement de données à caractère personnel effectués par les institutions et organes de l'UE, de donner des conseils sur les politiques et la législation qui touchent la vie privée, et de coopérer avec les autorités nationales homologues pour garantir une protection cohérente.

Le **Portugal** met également l'accent sur le rôle d'information des médias dans les débats sociétaux, qui est susceptible de compromettre le bon déroulement de certaines interventions des forces de l'ordre et de remettre en cause leur efficacité. Cela avait d'ailleurs été un débat en France lors des attentats de janvier 2015, lorsque des médias avaient diffusé des images et communiqués des informations en temps réel sur la conduite des opérations, sans se préoccuper de savoir si les terroristes avaient ou non accès à ces images et à ces informations.

Enfin, d'autres sujets de société, notamment mentionné par le **Royaume-Uni et les Pays-Bas,** tels que la radicalisation, le conservatisme religieux l'intégration des

communautés musulmanes, les inégalités de richesses à l'échelle internationale, la corruption sont énumérés dans les rapports comme les prochains sujets qui soulèveront les débats publics.