Vingt-cinq ans après le 11 septembre : qui décide aujourd'hui du seuil de surveillance acceptable ?

Créé le 09/09/2026· Dernière modification le 09/09/2026 · 16 min de lecture

Date

Le 09/09/2026

Chapô

This article is also available in English.

Vingt-cinq ans après les attentats du 11 septembre 2001, les démocraties continuent de s’interroger sur l’équilibre entre sécurité et libertés, alors même qu’une part croissante des décisions de sécurité s’est déplacée vers des acteurs privés. Ivan Manokha, professeur de relations internationales et de science politique à la Schiller International University de Paris, spécialiste de la surveillance, et enseignant à Sciences Po, revient sur ces enjeux pour montrer comment le 11-Septembre a moins constitué une rupture qu’une étape dans un lent processus de transformation des logiques de surveillance. Banques, compagnies aériennes, ou plateformes numériques étant désormais conduits à évaluer eux-mêmes les risques et à fixer certains seuils de précaution, qui est aujourd’hui responsable de décider jusqu’où la sécurité peut empiéter sur les libertés ?

Corps du texte

Vingt-cinq ans après les attentats du 11 septembre 2001, la question familière se pose : les démocraties ont-elles échangé trop de liberté contre la sécurité ? Ivan Manokha, professeur de Relations internationales et Politique à l'Université Schiller International à Paris, affirme que ce cadre de réflexion omet une transformation plus silencieuse mais tout aussi importante. Les années qui ont suivi le 11 septembre n'ont pas seulement étendu la surveillance et la sécurité préventive ; elles ont également transféré de nombreuses décisions de sécurité vers des entités privées telles que les banques, les compagnies aériennes, les sociétés de télécommunications et les plateformes numériques. Lorsque les autorités publiques fixent l'environnement du risque mais que les organisations privées décident où placer le curseur dans les cas individuels, qui est responsable de décider du seuil de précaution acceptable ?

L'expansion de la surveillance d'État

Il existe une manière familière de raconter l'histoire des vingt-cinq dernières années. Le 26 octobre 2001, six semaines après les attentats, la Loi PATRIOT américaine a été signée. La Grande-Bretagne a adopté la Loi sur l'antiterrorisme, le crime et la sécurité avant la fin de la même année. La France, qui avait déjà développé un arsenal substantiel de lutte antiterroriste à partir du milieu des années 1980, a ajouté d'autres mesures et, après les attentats de novembre 2015, a vécu sous état d'urgence jusqu'en novembre 2017. En juin 2013, les documents divulgués par Edward Snowden ont révélé l'ampleur des programmes de surveillance menés par la National Security Agency et ses partenaires des Five Eyes. Selon ce récit, le développement central après 2001 a été une expansion du pouvoir d'État, et cet anniversaire nous invite à nous demander si les démocraties ont accepté trop de surveillance en échange de la sécurité.

Ce récit est exact, mais il demeure incomplet. La transformation consécutive à 2001 a également été institutionnelle : la sécurité a de plus en plus été produite par des organisations dont la fonction première n'était pas la sécurité, par exemple les banques, le transport, les télécommunications ou la communication numérique. Certes, cela n'a pas commencé le 11 septembre ; les règles de lutte contre le blanchiment de capitaux s'appuyaient déjà sur les banques, et les règles de responsabilité des transporteurs en Europe préexistaient aux attentats.

Ce qui a changé après 2001, c'est la centralité de cette forme de gouvernance et, surtout, ce nouveau type de tâches que les organisations privées ont été amenées à accomplir. On attendait d'elles qu'elles identifient les risques, interprètent les signaux incertains et agissent avant que l'événement redouté ne se produise.

La sécurité s'est implantée dans les organisations ordinaires

Considérons ce qui s'est passé dans le secteur financier. Le Titre III de la Loi PATRIOT a imposé des obligations importantes aux institutions financières, notamment des exigences d'identification des clients et de nouveaux arrangements pour le partage d'informations. Le 28 septembre 2001, le Conseil de sécurité des Nations unies a adopté la Résolution 1373, exigeant des États qu'ils gèlent les actifs terroristes et empêchent les fonds d'être mis à la disposition de ceux impliqués dans des actes terroristes. Un mois plus tard, les 29 et 30 octobre, le Groupe d'action financière s'est réuni à Washington et a étendu son mandat au financement du terrorisme, en adoptant Huit Recommandations spéciales. Ces mesures s'adressaient formellement aux États, mais beaucoup de leur mise en œuvre pratique dépendait des banques, des sociétés de transfert d'argent et d'autres acteurs privés qui identifiaient les clients, suivaient les transactions, signalaient les soupçons et bloquaient l'accès aux fonds.

La même architecture s'est graduellement généralisée ailleurs : les compagnies aériennes collectent les informations sur les passagers qui sont transférées aux autorités publiques pour le contrôle de sécurité en vertu d'arrangements tels que le système d'enregistrement des passagers UE-États-Unis ; le régime de conservation des données européen adopté en 2006 exigeait que les prestataires de communications conservent les données de trafic et de localisation afin que les autorités compétentes puissent les obtenir dans les circonstances spécifiées, bien que la Cour de justice de l'UE ait invalidé cette directive en 2014. Plus récemment, les règles européennes sur le contenu terroriste en ligne exigent que les plateformes suppriment le matériel identifié dans un ordre de suppression dans un délai d'une heure et, dans certaines circonstances, adoptent des mesures supplémentaires de leur propre initiative. L'État n'a pas réellement disparu : il édicte des lois, émet des ordres et conserve des pouvoirs coercitifs ; cependant, le moment où une personne est classée, signalée, refusée ou supprimée se trouve de plus en plus à l'intérieur d'une organisation formellement privée.

Il est important de souligner ici une distinction conceptuelle cruciale : une banque qui ferme un compte ou une compagnie aérienne qui refuse l'embarquement n'est pas, en soi, un acte de surveillance (la surveillance concerne la collecte et le traitement de l'information), tandis que l'exclusion est une action entreprise sur la base de cette information. Cependant, l'architecture d'après 2001 connecte de plus en plus les deux : les organisations privées collectent ou conservent des données, classent une personne ou une transaction comme risquée, puis décident si l'accès doit continuer. Si nous regardons seulement qui « surveille », nous manquons la question tout aussi importante de qui est autorisé, formellement ou informellement, à agir sur les résultats de la surveillance.

Marieke de Goede a décrit ce développement par l'idée d'une « chaîne de sécurité », dans laquelle des entreprises qui ne se considèrent pas comme des organisations de sécurité font néanmoins des jugements de sécurité sur la base de données commerciales ordinaires. Le mot « jugement » est clé ici : une banque n'est pas simplement invitée à geler un compte après qu'un tribunal a établi que son propriétaire a financé le terrorisme ; on lui demande aussi de décider si un client, un transfert ou une relation présente un risque avant qu'une telle détermination n'existe. Il en va de même, de différentes manières, lorsqu'une compagnie aérienne évalue

les documents, qu'une plateforme décide si un contenu entre dans une catégorie interdite, ou qu'un employeur interprète un résultat de contrôle. La sécurité s'implante dans les routines organisationnelles ordinaires parce que la prévention exige que quelqu'un décide dans l'incertitude.

Les acteurs privés sont invités à juger le risque à l'avance

C'est ici que le vocabulaire de Michel Foucault est utile. Foucault affirme que le pouvoir n'opère pas seulement par les commandements ou les interdictions ; il peut aussi structurer le champ dans lequel d'autres prennent leurs propres décisions, en particulier en ce qui concerne l'obéissance, la conformité et l'autodiscipline. Appliqué ici, ce qui importe n'est pas que l'État se retire et que les entreprises privées deviennent souveraines ; c'est que les autorités publiques peuvent façonner la conduite de ces dernières en modifiant les risques que les organisations croient affronter.

Par exemple, une autorité bancaire n'a pas besoin de dire à une banque de résilier un client particulier ; elle peut publier une évaluation, placer une juridiction sur une liste, annoncer une priorité d'application ou imposer une lourde pénalité dans une autre affaire. La banque se pose alors une question différente de celle qu'un tribunal poserait : non pas simplement si ce client est actuellement interdit, mais si poursuivre la relation pourrait plus tard être décrite comme une preuve de contrôles inadéquats. Parce que les conséquences de la sous-réaction peuvent être graves, tandis que les conséquences réglementaires du refus d'activités marginales ou d'un compte individuel sont généralement beaucoup plus faibles, la précaution tend à se déplacer en direction du « sur-respect ».

Une bonne illustration en est le phénomène appelé « dérisquage financier ». Ce terme désigne l'interruption ou la restriction des relations avec les clients ou les catégories de clients afin d'éviter – plutôt que de gérer – le risque. Cela s’explique par plusieurs causes, telles que la rentabilité, les exigences prudentielles et les préoccupations de réputation, et il serait inexact d'attribuer chaque fermeture de compte à la politique antiterroriste. Néanmoins, le risque d'application des règles est une partie importante de la structure. Par exemple, en 2013, Barclays a annoncé qu'elle fermerait de nombreux comptes détenus par des entreprises de transfert d'argent, y compris des entreprises servant la Somalie, après avoir durci les critères selon lesquels elle était disposée à fournir des services bancaires au secteur. Ce qui est significatif ici, c'est qu'aucune autorité publique n'avait ordonné un retrait généralisé des entreprises de remises somaliennes ; la banque réagissait à sa propre évaluation des risques juridiques, réglementaires et réputationnels potentiels futurs de son maintien sur le marché. Cet épisode est particulièrement révélateur car le Groupe d'action financière lui-même a par la suite senti le besoin de clarifier ce que ses normes signifiaient, pour minimiser ces effets. En octobre 2014, il a déclaré explicitement que son approche fondée sur le risque exigeait une gestion du risque au cas par cas, non l'interruption généralisée de catégories entières de clients. En d'autres termes, l'organisme international dont les normes ont aidé à structurer l'environnement de conformité s'est trouvé expliquer que les acteurs privés en faisaient plus que les normes n'exigeaient.

Bien que les autorités ne veuillent pas nécessairement du sur-respect et puissent même tenter de l'éviter, dans cet environnement, les acteurs privés sentent que la prudence est plus récompensée. En effet, un agent de conformité qui approuve une relation crée un jugement qui pourrait plus tard s'avérer gravement dommageable si quelque chose tourne mal, tandis qu'une décision de refuser la relation peut imposer un coût très grave au client,

mais elle crée ordinairement beaucoup moins d'exposition réglementaire et de dommages pour l'institution. Les deux erreurs possibles ne sont donc pas évaluées de manière égale : la précaution est générée par la position dans laquelle l'organisation se trouve, pas nécessairement par une instruction d'être excessivement prudente.

Le travail de Didier Bigo sur le champ transnational des professionnels de la sécurité aide à placer ce développement dans un contexte plus large. La sécurité est produite non seulement par d'éminentes décisions souveraines mais aussi par les pratiques ordinaires de classification, de tri et de gestion des risques. Ce que les décennies après 2001 ont ajouté, c'est une interface de plus en plus dense entre ce champ de la sécurité et l'économie privée. Les personnes qui prennent des jugements de sécurité conséquents incluent maintenant les agents de conformité, les gestionnaires de risques, les analystes de données et les équipes de modération de contenu qui pourraient, de fait, ne jamais se qualifier eux-mêmes de professionnels de la sécurité.

Le modèle s'est étendu au-delà du contre-terrorisme

Il serait tentant de dire que le 11 septembre a créé ce modèle et qu'il s'est propagé par la suite, mais l'histoire est plus complexe que cela. La responsabilité des transporteurs dans le contrôle migratoire européen, par exemple, préexiste aux attentats : les compagnies aériennes et autres transporteurs étaient déjà tenus de vérifier si les voyageurs possédaient les documents nécessaires pour l'entrée et pouvaient être pénalisés pour le transport de passagers insuffisamment documentés. L'importance du 11 septembre réside ailleurs : il a contribué à faire que de tels jugements anticipés séparés ou occasionnels par des intermédiaires privés deviennent une façon normale d'organiser la sécurité, et le modèle s'est propagé à des questions bien au-delà du contre-terrorisme.

Ainsi, les sanctions financières fournissent un bon exemple. Après l'invasion de l'Ukraine par la Russie en février 2022, les entreprises se sont régulièrement retirées des transactions et des relations qui n'étaient pas elles-mêmes interdites, parce que les règles de sanctions étaient complexes, les structures de propriété étaient difficiles à établir et le coût d'une décision permissive incorrecte pouvait être très élevé. Les contrôles à l'exportation sur les technologies sensibles s'appuient de la même manière sur les fabricants, les distributeurs, les banques et les prestataires logistiques pour enquêter sur les contreparties et les utilisations finaux avant que les transactions ne se produisent. La règle juridique peut être publique, mais son périmètre d'application effectif est souvent tracé à l'intérieur de systèmes de conformité privés.

Les plateformes numériques constituent un autre exemple du même développement. Certains suppléments suivent des ordres juridiques directs, tandis que d'autres résultent des règles précautionnelles propres à la plateforme. Ces situations ne devraient évidemment pas être confondues, mais les préoccupations du public se traduisent souvent par des normes internes, des seuils automatisés et des catégories qui fonctionnent à une échelle qu'aucune autorité ne pourrait administrer au cas par cas. Une fois codifié dans un système privé, le signal public qui a contribué à produire la règle peut devenir difficile à voir, ce qui soulève à son tour des questions importantes concernant la responsabilité et la transparence face aux clients et aux utilisateurs qui peuvent être touchés par de telles décisions opaques.

Nous pouvons donc affirmer que la transformation d'après 2001 concerne une forme de raisonnement : elle est préventive plutôt que rétrospective, car elle agit sur ce qui pourrait se produire ; elle repose fortement sur les catégories et le tri à grande échelle, parce que les grandes organisations ne peuvent pas enquêter sur

chaque personne individuellement ; elle transfère une grande partie du coût d'interprétation et de contrôle aux intermédiaires privés. De plus, elle laisse souvent le seuil opérationnel – le point où un client devient trop risqué, une transaction trop incertaine ou un contenu trop dangereux – à être fixé par ces organisations elles-mêmes.

Le contrôle démocratique s'est fragmenté

Une collectivité démocratique dispose de mécanismes clairs pour débattre d'un décret ou d'une loi. Par exemple, après les attentats de novembre 2015, la France a déclaré l'état d'urgence (qui a été par la suite régulièrement prorogé), mais cette décision a été publiquement contestée et a finalement pris fin le 1er novembre 2017.
Il en va de même pour la loi sur la sécurité intérieure et le contre-terrorisme adoptée le 30 octobre, qui a introduit plusieurs mesures préventives en droit ordinaire. Que l'on considère cette décision comme nécessaire, excessive ou comme une normalisation inacceptable des pouvoirs d'urgence n'est que secondaire – ce qui importe, c'est que l'objet institutionnel est visible : il existe un texte, un historique parlementaire, une autorité publique responsable et des tribunaux capables d'en examiner les dispositions.
En contraste, l'arrangement décrit ci-dessus avec les acteurs privés adoptant leurs propres interprétations et décisions d'application est beaucoup plus difficile à débattre ou à réexaminer : un régulateur peut émettre un avertissement général, mais une banque peut le traduire en une politique de risque spécifique qui n'était pas prévue par le régulateur ; un fournisseur de logiciels peut intégrer une politique différente dans un système de contrôle et commencer à l'appliquer, ce qui n'était pas implicite dans l'avertissement général du régulateur. Ainsi, si elle est critiquée, le régulateur peut à juste titre dire qu'il n'a jamais ordonné la fermeture du compte, tandis que la banque peut correctement dire qu'elle a pris une décision commerciale. Aucune de ces affirmations n'est nécessairement évasive ; le problème est que la conséquence n'existe que parce que les deux formes d'action interagissent.

Maintenant, il serait également inexact de dire qu'il n'existe aucun recours du tout. En effet, les clients peuvent parfois se plaindre aux banques ou aux médiateurs, les utilisateurs peuvent faire appel des décisions des plateformes, et certains régimes réglementaires prévoient des droits de contestation. La difficulté réside ailleurs – dans la fragmentation croissante des décideurs et des mesures d'application. Un appel privé peut examiner si l'entreprise a suivi ses règles sans se demander si le signal public qui les a façonnées était trop large, tandis qu'un tribunal examinant l'autorité publique peut constater que l'autorité n'a jamais pris la décision individuelle contestée. Il peut y avoir plusieurs forums et toujours ne pas disposer d'un seul forum dans lequel l'ensemble de la chaîne soit visible.

À la lumière de ce qui précède, nous pouvons suggérer que c'est là l'une des questions les plus importantes – et les plus difficiles – que les démocraties doivent affronter vingt-cinq ans après le 11 septembre. La question liberté-contre-sécurité reste, bien sûr, indispensable, mais elle présuppose que nous sachions où la décision de sécurité est prise. De plus en plus, la réponse est qu'une partie en est prise par les autorités publiques et une partie à l'intérieur des infrastructures privées de conformité, de traitement des données et de gestion des risques. En d'autres termes, le seuil n'a pas simplement été abaissé : il a été distribué.

Certaines réformes et actions immédiates pourraient être suggérées : les autorités publiques peuvent commencer à mesurer et à publier les effets en aval de leurs avertissements, listes et priorités d'application ; les régulateurs peuvent corriger le sur-respect prévisible lorsqu'il devient visible plutôt que simplement d'insister

sur le fait que les entreprises devraient être plus proportionnées. Lorsque le droit de la sécurité le permet, les organisations peuvent donner des raisons significatives pour les exclusions importantes et prévoir un examen par une entité capable de reconsidérer le jugement de risque sous-jacent. Pour le redire, rien de cela n'exige de prétendre que la sécurité peut être organisée sans précaution, ou que les banques et les plateformes doivent ignorer les risques véritables. Ce qu'il faut, c'est rendre l'exercice de la précaution plus visible là où il acquiert les effets du pouvoir public.

En conclusion, l'une des leçons des vingt-cinq dernières années est donc non seulement que les démocraties ont choisi la sécurité plutôt que la liberté après le 11 septembre 2001. C'est qu'elles ont de plus en plus organisé la sécurité de façons qui permettent à des choix conséquents d'être pris en dehors des institutions dans lesquelles les sociétés démocratiques ont l'habitude de les débattre, de les contester et de les annuler. Le problème aujourd'hui n'est pas seulement que la ligne a bougé ; c'est que nous ne pouvons plus désigner une institution spécifique et lui demander de déplacer la ligne en arrière.

Voir aussi

https://conference.sciencespo.fr/playlist/4APsVpsvRXIWM15v3srI

Thématique

Démocratie | Numérique

Licence

Langue

Français

Auteur

Ivan Manokha

Avant de rejoindre Oxford en 2016, Ivan Manokha a enseigné à Sciences Po et, auparavant, à la London School of Economics et à l'Université du Sussex. Il est aujourd'hui professeur à temps plein en relations internationales et diplomatie à la Schiller International University et continue d'enseigner à Sciences Po ainsi qu'à l'IESEG School of Management. Dans ses recherches, Ivan Manokha a étudié la relation entre le capitalisme mondial et les droits individuels et, plus récemment, il s'est penché sur la question du pouvoir et de l'obéissance dans l'économie politique de la modernité tardive, en particulier dans le contexte du développement des nouvelles technologies de surveillance.