



# Surveillance, vie privée et sécurité

Votre avis nous intéresse !

**surprise**  
surveillance  
privacy  
security





# Table des matières

1	Bienvenue dans SurPRISE	5
1.1	Comment lire cette brochure	6
2	Résumé	7
3	Un jour ordinaire...	9
3.1	Surveillance, vie privée et sécurité	10
3.1.1	Surveillance	10
3.1.2	Vie privée et protection des données : des questions importantes ?	11
3.1.3	Sécurité	11
4	Trois nouvelles technologies de sécurité	13
5	La cybersurveillance par l'inspection approfondie des paquets (DPI)	15
5.1	Pourquoi a-t-on développé le DPI ?	15
5.2	Comment le DPI est-il utilisée ?	16
5.2.1	Utilisations commerciales	17
5.2.2	Utilisations pour la sécurité publique et nationale	18
5.3	Améliorations de la sécurité	18
5.4	Enjeux	19
6	La géolocalisation des smartphones	27
6.1	Pourquoi a-t-on développé la géolocalisation des smartphones ?	21
6.2	Comment la géolocalisation des smartphones est-elle utilisée ?	23
6.2.1	Utilisations commerciales	23
6.2.2	Utilisations pour la sécurité publique et nationale	24
6.3	Améliorations de la sécurité	24
6.4	Enjeux	25
7	La vidéosurveillance intelligente	27
7.1	Pourquoi a-t-on développé la vidéosurveillance intelligente ?	27
7.2	Comment la vidéosurveillance intelligente est-elle utilisée ?	28
7.3	Améliorations de la sécurité	30
7.4	Enjeux	30
8	La technologie est-elle la seule réponse ?	33
8.1	Solutions locales	33
8.2	Solutions nationales ou internationales	33
9	A vous maintenant !	35
	Au sujet de ce document	36



# 1 Bienvenue dans SurPRISE

Bienvenue dans SurPRISE, un projet de recherche réunissant plusieurs pays d'Europe. SurPRISE est l'abréviation de «Surveillance, Privacy and Security» («surveillance, vie privée et sécurité»). Son objectif est de recueillir les opinions du public européen sur les nouvelles technologies de sécurité. Nombre de ces technologies recourent à la surveillance de personnes et de leurs faits et gestes. Elles sont utilisées par la police ou le personnel de sécurité pour observer ce qui se passe, détecter et éviter des problèmes de sécurité. Lorsque vous allez dans un aéroport et que vos bagages sont contrôlés par un scanner, ou lorsqu'une caméra de vidéosurveillance enregistre l'activité de la rue le long de laquelle vous marchez, vous êtes en présence de technologies de sécurité basées sur la surveillance. Le but de SurPRISE est de s'assurer que ces technologies sont efficaces et sûres, et qu'elles respectent les droits de l'homme. Pour réaliser cet objectif, SurPRISE a besoin de votre aide.

Nous vous avons invité à participer au projet SurPRISE car la Commission européenne aimerait savoir ce que les citoyennes et citoyens pensent devoir être fait pour qu'ils soient et se sentent en sécurité. En participant au forum de discussion SurPRISE, vous pourrez échanger vos idées sur les nouvelles technologies de sécurité avec d'autres personnes. SurPRISE veut recueillir des opinions citoyennes au sujet de ces technologies et en faire part aux politiciens et politiciennes.

Des forums de discussion sont organisés dans neuf pays d'Europe : en Autriche, en Allemagne, au Danemark, en Espagne, en Hongrie, en Italie, en Norvège, au Royaume-Uni et en Suisse. Les résultats seront remis à l'Union européenne en juin 2014 et diffusés aux médias, aux autorités politiques et à la population.

La brochure que vous tenez entre les mains fournit des informations de base sur les questions qui seront discutées lors du forum du 22 mars 2014 à Grandson. Elle renseigne sur les

nouvelles technologies de sécurité étudiées par le projet SurPRISE et fournit des informations générales ayant trait à la surveillance, la sécurité et la vie privée en Europe. Vous y trouverez notamment des explications sur les enjeux de la géolocalisation des smartphones et sur le DPI (surveillance d'internet par l'inspection approfondie des paquets de données), deux technologies qui seront discutées à Grandson.

Nous savons que la lecture de cette brochure représente un effort important. Mais nous n'allons pas tester ce que vous savez et n'avons pas l'intention de faire de vous un expert ! Le but de la brochure est de vous donner une idée des questions qui seront discutées lors du forum et de vous faire réfléchir à votre opinion personnelle en matière de surveillance, de vie privée et de sécurité. C'est précisément parce que vous n'êtes pas un expert que votre participation au forum de discussion est importante. Nous vous avons invité à y prendre part parce que vous êtes un «simple citoyen» ou une «simple citoyenne» et que les décisions prises par les politiciens ont une incidence sur votre vie quotidienne.

SurPRISE transmettra vos opinions de citoyens et de citoyennes aux décideurs de manière anonyme. Les technologies de sécurité sont en rapport avec les droits de l'homme, la justice et l'équité, et avec l'efficacité des institutions et la confiance qu'on peut leur témoigner. C'est pourquoi les débats à leur sujet doivent inclure le grand public et pas seulement les responsables politiques, les industries, les experts et les organisations caritatives. Les politiciens définissent la politique de sécurité, mais vous en tant qu'individu devrez vivre avec les conséquences de ces décisions. C'est cela qui rend votre opinion si importante.

**La science nous informe. Elle ne nous dit pas ce qu'il faut faire. C'est à nous de choisir. A vous la parole !**

## 1.1 Comment lire cette brochure

Cette brochure comprend cinq parties principales. La première partie est une introduction générale sur la surveillance, la sécurité et la vie privée en Europe. Les trois chapitres qui suivent donnent un aperçu des technologies de sécurité que nous discuterons lors du forum de discussion. Bien que la brochure aborde trois technologies, deux d'entre elles seulement seront discutées lors du forum, à savoir la géolocalisation des smartphones et la cybersurveillance par DPI (inspection approfondie des paquets).

Chacun de ces chapitres décrit pourquoi la technologie a été développée, comment elle est utilisée, en quoi elle améliore la sécurité et quelles sont ses limites. Dans chacun des chapitres dédiés à une technologie, nous avons inclus un encadré expliquant plus en détail comment elle fonctionne, ainsi qu'un encadré exposant une controverse qu'elle suscite. La dernière partie discute brièvement des alternatives aux technologies de sécurité.

Si vous ne souhaitez pas lire tout le document, nous vous proposons dans les pages suivantes un résumé présentant les points principaux.

## 2 Résumé

SurPRISE a pour but de révéler la diversité des opinions des citoyennes et citoyens européens sur les nouvelles technologies de sécurité. Les gouvernements européens étant de plus en plus préoccupés par le terrorisme, le crime organisé et la cybercriminalité, ils ont investi dans le développement de nouvelles technologies de sécurité.

Nombre de ces technologies analysent l'information générée par des citoyennes et citoyens durant leur vie quotidienne. Elles se servent d'informations provenant, par exemple, des téléphones mobiles, de l'internet et de technologies intelligentes telles que la vidéosurveillance numérique pour essayer d'identifier des criminels et des terroristes, parfois avant qu'ils agissent.

Du fait que ces technologies utilisent des informations personnelles, nous les appelons «technologies de sécurité basées sur la surveillance».

Une technologie de sécurité basées sur la surveillance est...

*...une technologie qui s'attaque à un problème de sécurité en se servant d'informations recueillies dans différents contextes sur la population en général et ses activités.*

Lors des forums de discussion SurPRISE, les participants examineront en détail trois de ces technologies (mais seulement deux par pays) :

- > **La vidéosurveillance intelligente:** Elle recourt à des systèmes de vidéosurveillance qui vont au-delà de la simple observation d'espaces publics. La vidéosurveillance intelligente fait appel à des caméras numériques reliées entre elles dans un système qui peut reconnaître le visage de personnes, analyser leur comportement et détecter des objets.
- > **La cybersurveillance par le DPI (inspection approfondie des paquets de données transitant par internet) :** Des dispositifs matériels et des logiciels spécialisés permettent de lire, analyser et modifier tous les messages et informations transmis par l'internet.
- > **La géolocalisation des smartphones :** L'analyse de données de localisation provenant d'un téléphone mobile permet de recueillir des informations sur la position et les déplacements de l'utilisateur de l'appareil pendant une période donnée. Le téléphone peut être localisé par des données

provenant des antennes relais auxquelles l'appareil s'est connecté, et de façon plus précise par le système de positionnement mondial (GPS) ou par des données transmises sans fil.

Chacune de ces technologies peut améliorer la sécurité en détectant des suspects et des activités criminelles ou illégales. D'aucuns pensent que ces technologies peuvent aussi faciliter grandement la vie. Mais chacune d'elles a une série d'inconvénients. Par exemple, la vidéosurveillance intelligente ne fonctionne que dans certaines conditions et peut produire de nombreuses fausses alarmes. Le DPI compromet le caractère privé des communications en ligne. La géolocalisation des smartphones est difficile à contrôler, parce que de nombreuses applications transmettent des informations de localisation à partir de l'appareil à l'insu de son utilisateur. Le manque de contrôle sur la collecte et l'utilisation d'informations est un problème associé à toutes les technologies que nous examinons.

En dépit de l'amélioration potentielle que ces technologies offrent en termes de sécurité, certaines personnes sont mitigées quant à l'utilisation de leurs informations à des fins de sécurité. S'il en résulte plus de sûreté pour chacun, c'est peut-être une bonne chose. Mais si des droits humains fondamentaux sont enfreints, ça peut devenir inacceptable. Les opinions varieront d'une personne à l'autre, en fonction de l'idée qu'elles se font sur divers aspects en question, comme par exemple :

- > Ces technologies fonctionnent-elles vraiment ?
- > A quelle point sont-elles intrusives ?
- > Les institutions qui s'en servent sont-elles dignes de confiance ?
- > La réglementation en vigueur est-elle efficace et suffisante ?
- > Qui surveille les surveillants ?
- > Quelles sont les alternatives et sont-elles praticables ?

Telles sont quelques-unes des questions que nous discuterons pendant le forum SurPRISE.

**Si vous voulez en savoir davantage sur ces questions, nous vous invitons à poursuivre la lecture.**





## 3 Un jour ordinaire...

Au sud de Budapest, Aisha s'engage sur la route E-75 pour se rendre à l'aéroport international de Ferihegy. Elle se souvient de la première fois qu'elle a emprunté cette route. Elle s'était acquittée du péage routier sur place : maintenant, il est débité automatiquement de son compte bancaire. Son numéro minéralogique est saisi par les caméras de lecture automatique des plaques d'immatriculation (LAPI) et le système de péage routier fait le reste. Auparavant, Aisha n'avait pas constaté la présence de caméras. Maintenant, elle les voit et se demande comment l'information est communiquée à la banque.

Aisha parque sa voiture et monte à bord de la navette conduisant au terminal. Là, elle s'enregistre pour son vol à une borne d'enregistrement en libre-service. Elle pose son passeport sur l'appareil, lequel apparie son nom avec les détails de la réservation. Tandis qu'elle reçoit sa carte d'embarquement, Aisha réalise que des informations à son sujet sont stockées quelque part.

Après avoir passé le contrôle, Aisha s'arrête à un snackbar et pose son bagage à main par terre. Elle commande un café, mais marque un temps d'arrêt avant de tendre sa carte de débit au caissier. «Ce bout de plastique est bien pratique, pense-t-elle, mais qui enregistre la transaction et comment ?»

En attendant que son café refroidisse, Aisha sort son smartphone pour voir s'il y a des messages. Alors que l'écran commence de s'animer, le lieu affiché sur la page d'accueil change aussitôt de «Kecskemét», où Aisha habite, à «Ferihegy». «Comment sait-il cela ? Il doit y avoir une explication toute simple, se dit-elle, mais je ne vois pas laquelle».

Aisha a juste un moment pour envoyer un courriel à un collègue de travail avant qu'il soit temps de monter à bord. Tandis qu'elle met son téléphone en mode avion, elle se demande ce qui se va se passer avec son courriel tout au long de son parcours à travers l'internet.

L'histoire d'Aisha n'a rien d'inhabituel et est commune à tous les voyageurs. Les technologies offrent des avantages à Aisha, en lui permettant de voyager plus facilement et plus efficacement. Mais des questions lui viennent à l'esprit : «qui se sert de mes informations personnelles et que signifie pour moi qu'elles soient dans le système ?»

Nombre de technologies qu'Aisha a rencontrées jouent un rôle important aussi en dehors du monde des aéroports. Beaucoup de gens ne pourraient pas imaginer vivre sans leur smartphone, leur carte bancaire ou l'internet ! En fait, de nombreuses activités quotidiennes génèrent le genre de données électroniques dont Aisha a pris conscience. Vous vous posez peut-être les mêmes questions qu'elle. Ces données peuvent indiquer où nous sommes dans l'espace et dans le temps, et parfois même ce que nous faisons. Par exemple, des transactions bancaires, y compris celles effectuées par cartes de débit, peuvent révéler les types d'achats que nous effectuons et avec qui nous sommes en relation. Ces informations sont conservées dans des bases de données bancaires et figurent sur nos relevés de comptes.

Les informations que les compagnies aériennes détiennent sur les réservations de vols peuvent indiquer si nous voyageons vers ou depuis une région à risque. Les données de téléphonie mobile indiquent le lieu où nous nous trouvons, avec qui nous parlons et combien de fois nous le faisons. Ces informations sont détenues par les opérateurs de téléphonie mobile et les fournisseurs de services internet dans leurs bases de données. La réglementation européenne impose que ces informations soient conservées pendant au moins six mois et jusqu'à deux ans. Ceci permet d'identifier, suivre et rechercher la plupart des gens à différents moments de leur vie. C'est peut-être cela qui inquiète Aisha, mais elle est partagée, car ces technologies lui offrent aussi de nombreux avantages.

Des technologies telles que celles discutées plus haut et les informations qu'elles collectent peuvent procurer des avantages aussi à des tiers. A la suite d'attentats terroristes de grande envergure en Europe et ailleurs, les Etats ont investi dans des technologies de pointe qui utilisent ce genre d'informations. Ils ont aussi modifié des lois existantes et en ont adopté de nouvelles pour permettre l'accès à ces informations à des fins de sécurité.

Bien qu'il existe de nombreuses sources «officielles» de renseignements, les Etats ont réalisé qu'il pourrait y avoir encore d'autres moyens de détecter les activités de criminels et terroristes présumés. Comme la majorité des citoyens, les criminels et les terroristes ont des comptes bancaires, possèdent des documents d'identité, se servent de l'internet et ont des téléphones portables. Ils utilisent les systèmes de transport, les espaces publics et consomment des biens et des services. En savoir plus sur ces activités peut constituer une source d'indices pour trouver des criminels et des terroristes. Nombre de gouvernements pensent qu'en recourant à de nouvelles technologies de sécurité, il sera possible non seulement d'arrêter des malfaiteurs, mais aussi de les identifier avant qu'ils ne fassent du mal. Dans le projet SurPRISE, les technologies qui utilisent des informations à cet effet sont appelées «technologies de sécurité basées sur la surveillance».

Une technologie de sécurité basée sur la surveillance est...

*...une technologie qui s'attaque à un problème de sécurité en se servant d'informations recueillies dans différents contextes sur la population en général et ses activités.*

Si Aisha prenait en considération que ses informations peuvent être utilisées de cette manière, serait-elle encore hésitante ? Peut-être admettrait-elle qu'il en soit ainsi si cela signifie davantage de sécurité pour elle et les autres. Cependant, le recours à ces technologies soulève des questions de droits humains, de respect de la vie privée, de réglementation et de confiance. Généralement, ces technologies recueillent et partagent des informations sur une personne sans qu'elle le sache. Il est donc inévitable qu'elles saisissent et analysent également des données sur des innocents ; certaines le font même délibérément. En tant que telles, ces technologies peuvent être une atteinte à la vie privée, qui est un droit humain fondamental, protégé en Europe. Des innocents peuvent même être identifiés à tort comme malfaiteurs par ces technologies, avec les graves conséquences que cela implique pour leur vie.

Une série de questions surgissent :

- > Les institutions qui se servent de ces données sont-elles dignes de confiance ?
- > Dans quelle mesure ces institutions sont-elles réglementées ?
- > Les technologies sont-elles utilisées conformément à la loi ?
- > Les institutions font-elles preuve de transparence et doivent-elles rendre des comptes pour les atteintes à la vie privée commises au nom de la sécurité ?
- > Ces technologies améliorent-elles vraiment la sécurité ?

Ce sont là quelques-unes des questions qui seront examinées lors du forum de discussion.

Dans les paragraphes suivants, nous présentons quelques termes et définitions clés, avant de décrire les technologies que nous regarderons de près pendant les discussions.

## 3.1 Surveillance, vie privée et sécurité

### 3.1.1 Surveillance

Quand vous pensez à la surveillance, il est probable que quelques images nous viennent aussitôt à l'esprit : vous pensez peut-être à «Loft Story», la série de télévision réalité, ou à Big Brother, le personnage du roman 1984 de George Orwell. Il se peut alors que la surveillance éveille en vous le sentiment angoissant d'être observé par une personne ou une organisation puissante mais inconnue.

Lorsque nous parlons de «surveillance» dans SurPRISE, nous pensons à un «contrôle de personnes pour réguler ou régir leur comportement», ceci pouvant être entrepris dans différents buts. La surveillance peut avoir lieu à des fins de sécurité. Par exemple, la police peut faire appel à la vidéosurveillance pour repérer des malfaiteurs dans la rue. La surveillance peut aussi avoir des buts commerciaux. Par exemple, un supermarché peut recourir à des cartes de fidélité pour connaître les préférences d'achats de différents groupes de clients et par la suite mieux cibler les offres spéciales qui leur sont

adressées. La surveillance peut donc servir à prévenir des délits et à arrêter des criminels, mais elle intervient aussi pour proposer aux consommateurs des produits et des services.

Si la surveillance fait partie du cours normal de la société, vous vous demandez peut-être où est le problème. Dans les articles de presse, la «société de surveillance» semble toujours avoir quelque chose d'inquiétant. Le fait est qu'avoir le contrôle d'une technologie de surveillance confère un grand pouvoir à qui en a le contrôle. Il importe que ceux qui le détiennent, par exemple les forces de l'ordre, des courtiers en données ou des entreprises de distribution, usent de ce pouvoir avec honnêteté et dans le respect des libertés civiles et de la loi.

Si vous pensez n'avoir rien à cacher ni rien à craindre dépend en réalité de qui vous observe, de pourquoi on vous observe, et de comment vos actions sont perçues. Si vous n'avez aucun contrôle ni rien à dire dans ce processus et que les règles changent en votre défaveur – peut-être en raison de votre appartenance ethnique, de votre religion, de votre orientation sexuelle, de votre sexe ou de vos opinions politiques – que ferez-vous ? Une surveillance excessive peut avoir un impact négatif sur d'autres droits humains, tels que la liberté d'expression. Dans ces circonstances, la surveillance peut aussi porter atteinte à la confiance sociale, les gens ayant peur d'être eux-mêmes. Beaucoup de choses sont en jeu lorsque différentes formes de données de surveillance sont utilisées dans le contexte de la sécurité.

### 3.1.2 Vie privée et protection des données : des questions importantes ?

L'une des principales questions en jeu concerne la vie privée et la manière dont les données produites et utilisées par les nouvelles technologies de sécurité sont sécurisées. Bien que la sphère privée ne signifie pas la même chose pour tout le monde, elle a une grande importance dans la vie de tous les jours. Il y a un certain nombre de choses que vous souhaitez garder privées à différentes occasions :

- > ce que vous faites, pensez et ressentez ;
- > des informations sur vos relations intimes, l'endroit où vous êtes, ce que vous communiquez à d'autres par la poste ou par

courriel, vos caractéristiques personnelles et votre image ;

- > votre corps : ce que vous voulez en révéler, pouvoir le préserver d'attouchements non désirés ou de fouilles corporelles et garder le contrôle sur l'accès par des tiers à des constituants de votre corps tels que votre ADN ou vos empreintes digitales.

Réfléchissez : seriez-vous heureux que votre compagnie d'assurance-vie ait un accès illimité à vos données médicales ? Ou que la police puisse écouter tous vos appels téléphoniques ? Avez-vous des rideaux dans votre maison ? Si vous avez répondu «non» aux deux premières questions et «oui» à la troisième, vous vous inquiétez encore de votre vie privée ! Et ce n'est pas seulement vous. Des enquêtes menées auprès de jeunes personnes utilisant des médias sociaux ont montré qu'ils ne divulguent des informations sur eux-mêmes que de façon très sélective, afin de préserver leur vie privée. Les gens ont toujours envie de partager des informations, mais ils veulent le faire dans des limites bien établies. Pour les individus, tout ce qui est au-delà de ces limites représente les zones de leur vie qu'ils entendent maintenir à l'abri d'interférences avec l'extérieur : leur vie privée.

Dans SurPRISE, nous définissons la vie privée comme...

*...la capacité pour un individu d'être laissé en paix, loin des regards du public, et de contrôler les informations le concernant.*

Le droit à la vie privée et le droit à la protection de ses données personnelles sont des droits humains fondamentaux dans l'Union européenne. Chacun a besoin du droit à la vie privée : pour être libre d'agir, de rencontrer des gens et de discuter dans une société démocratique. Les gens ne peuvent pas exercer leurs libertés démocratiques si tout est su sur leurs pensées, intentions et actions. Les nouvelles lois européennes sur la protection des données insistent de plus en plus sur le fait d'intégrer le respect de la vie privée dans la conception des nouvelles technologies, pour les rendre dès le départ moins intrusives. Les entreprises de high-tech sont encouragées à prendre en compte la protection de la vie privée à chaque étape de leur activité. Cette nouvelle approche, appelée en anglais «privacy by design», entend promouvoir le respect de la vie privée dès la conception d'une technologie.

### 3.1.3 Sécurité

Dans le projet SurPRISE, nous définissons la sécurité comme...

*...l'état selon lequel nous sommes protégés contre tout danger ou n'y sommes pas exposés ; un sentiment de sécurité ou d'absence de danger.*

La sécurité ne concerne pas seulement la protection d'objets physiques, tels que bâtiments, systèmes d'information, frontières nationales, etc., mais inclut aussi le fait de se sentir en sécurité. Dans l'idéal, des mesures efficaces de sécurité devraient augmenter le sentiment de sécurité, mais cela n'est pas toujours le cas.

Il semble étrange de penser que parce que les nouvelles technologies de sécurité peuvent affecter notre vie privée, elles pourraient finir par nous faire sentir moins sûrs, alors même qu'elles devraient nous faire sentir plus sûrs. Mais ce sentiment peut varier d'une personne à l'autre. Comme la vie privée, la sécurité signifie des choses très différentes pour différentes personnes. Nous avons chacun notre propre perception de ce que nous considérons être une menace pour la sécurité et de ce que nous sommes prêts à faire pour protéger les choses qui sont importantes pour nous.

Ceci est vrai aussi pour ceux qui sont en charge de la sécurité. Ils doivent identifier et traiter les menaces les plus importantes. Tout gouvernement a des ressources économiques, humaines et techniques limitées à consacrer à la sécurité et doit donc faire des choix. Pour l'Union européennes, les priorités en matière de sécurité sont :

- > augmenter la cybersécurité des citoyennes et citoyens et des entreprises ;
- > démanteler les réseaux criminels internationaux ;
- > prévenir le terrorisme ;
- > accroître la capacité de l'Europe à se remettre de toutes sortes de crises et de désastres.

L'Europe ayant décidé de mettre l'accent sur sa capacité de récupération après toutes sortes de crises et de désastres, son concept de sécurité va au-delà de la prévention du crime et du terrorisme. L'Europe se préoccupe aussi de menaces sur l'environnement, les ressources naturelles, les infrastructures, les activités économiques et la santé. Pour les responsables politiques, la sécurité s'est étendue à presque tous les domaines de la vie publique. Cette approche a été adoptée par de nombreux Etats européens. Mais la promesse de sécurité dans tous ces domaines peut-elle être satisfaite ? L'industrie de la sécurité gagne en importance et se développe en Europe pour répondre à ce besoin. Elle comprend de grandes sociétés de défense, telles qu'Airbus, BEA Systems et Finmeccanica, et de nombreuses entreprises plus petites. Les récents développements en matière de technologies de sécurité basées sur la surveillance incluent :

- > la vidéosurveillance intelligente, axée sur le repérage de délinquants connus et la détection de comportements suspects ;
- > la cybersurveillance, qui vise à prévenir des dommages causés par des virus, hackers ou voleurs d'identité ;
- > la biométrie, qui est mise en œuvre pour prévenir l'entrée d'individus indésirables sur un territoire et accélérer le passage de ceux que les autorités connaissent comme étant des voyageurs auxquels on peut faire confiance ;
- > les drones de surveillance aérienne, qui permettent de repérer à partir des airs des activités dangereuses qui ne pourraient pas être vues du sol. Ces informations peuvent servir à diriger le personnel de sécurité vers des points chauds émergents ;
- > des systèmes avancés d'information sur les passagers, visant à détecter avant leur voyage des individus qui pourraient poser un problème ;
- > des technologies de localisation, destinées à minimiser les atteintes matérielles à des choses en mouvement et à localiser avec précision des suspects dans l'espace physique.

# 4 Trois nouvelles technologies de sécurité

Les trois technologies de sécurité examinées par le projet SurPRISE sont :

- > **la cybersurveillance par DPI (inspection approfondie des paquets)**
- > **la géolocalisation des smartphones**
- > **la vidéosurveillance intelligente**

Ces technologies de sécurité continuent de se développer et il est encore possible de préciser les politiques et mesures les concernant.

Dans les chapitres suivants, nous expliquons comment chacune de ces technologies fonctionne, pourquoi elle a été développée,

qui s'en sert et comment elle est utilisée. Nous décrivons aussi en quoi elles améliorent la sécurité et abordons les enjeux de vie privée ainsi que d'autres questions liées à leur utilisation.

Il est important pour ce projet, et pour l'Union européenne, de savoir ce que les gens pensent des technologies de sécurité et dans quelle mesure ils les trouvent acceptables. C'est pour cela que nous tenons tant à connaître votre opinion. Vous êtes peut-être déjà résolument pour ou contre certaines de ces technologies. Durant le forum de discussion SurPRISE, vous aurez maintes fois l'occasion d'exprimer votre opinion, mais nous aimerions vous inviter à réfléchir en particulier aux questions suivantes.

## Qu'est-ce qui rend une technologie de sécurité plus ou moins acceptable pour vous ?

Serait-ce :

- > En savoir plus sur la technologie en question et son fonctionnement ?
- > En savoir plus sur les institutions qui se servent de cette technologie et sur les informations qu'elle produit ?
- > Avoir une réglementation efficace et des mécanismes de contrôle ?
- > Être mieux informé sur les types de menaces auxquels nous sommes confrontés actuellement et contre lesquels cette technologie est mise en œuvre ?

Ou cela dépend-il de votre appréciation du degré d'intrusion de cette technologie ? Par exemple :

- > Cause-t-elle des ennuis ?
- > Porte-t-elle atteinte à des droits fondamentaux ?
- > Révèle-t-elle à votre insu des informations à des tiers, ou a-t-elle un impact sur d'autres aspects de votre vie privée ?

Cela tient-il au niveau d'efficacité de la technologie :

- > Facilite-t-elle la vie ?
- > Vous procure-t-elle le sentiment d'être plus en sécurité ?
- > Identifie-t-elle à votre avis des suspects avec précision ?

Ou pensez-vous aux technologies de sécurité seulement quand vous les sentez physiquement près de vous, par exemple dans un aéroport, dans la rue, ou lorsque vous utilisez un téléphone mobile ou l'internet ? Le reste du temps, elles ne vous tracassent pas. Peut-être que les technologies de sécurité sont acceptables pour vous aujourd'hui, mais que vous vous inquiétez de leur utilisation future.





## 5 La cybersurveillance par l'inspection approfondie des paquets (DPI)

Alors qu'elle était assise au snackbar de l'aéroport, Aisha se demandait ce qui allait se passer avec le courriel qu'elle venait d'envoyer à son collègue. Pendant son parcours à travers l'internet, son message pourrait fort bien avoir affaire à une technique de cybersurveillance appelée DPI (Deep Packet Inspection ou, en français, inspection approfondie des paquets).

Les fournisseurs de services internet, les opérateurs de télécoms et les sociétés de télécommunications ont toujours été en mesure de contrôler leurs réseaux. Savoir qui communique avec qui, quels sites web sont visités et quels services sont utilisés offrent autant d'informations utiles pour la facturation des clients, la gestion du réseau et les activités de marketing de ces sociétés. Toutefois, une technique appelée «inspection approfondie des paquets» (ou DPI pour Deep packet inspection) permet aux sociétés, services de renseignements et gouvernements de lire le contenu des communications envoyées par l'internet. Pour faire une analogie, le DPI équivaut à l'activité de la poste qui ouvrirait les lettres, les lirait et déciderait parfois d'en modifier ou effacer le contenu, ou de ne pas les livrer du tout. Le DPI permet de suivre de près tous les aspects des communications numériques. Cela va des informations que vous lisez en ligne, des sites web que vous visitez, des vidéos que vous regardez et de vos termes de recherches, jusqu'aux personnes avec lesquelles vous communiquez par courriel, à la messagerie instantanée ou aux médias sociaux. Les applications du DPI détectent et influencent la manière selon laquelle des messages circulent dans un réseau. Elles ouvrent et analysent les messages pendant qu'ils voyagent et identifient ceux qui posent un risque particulier. Tout le monde est concerné par le DPI, pas besoin d'être suspect – le DPI intercepte et lit tous les messages qui circulent sur le réseau d'un fournisseur de services internet.



### 5.1 Pourquoi a-t-on développé le DPI ?

A l'origine, le DPI a été développé pour détecter des virus et autres logiciels malveillants susceptibles d'endommager des réseaux d'ordinateurs. Aujourd'hui, le recours au DPI pour analyser le contenu de messages pendant qu'ils voyagent permet non seulement d'intercepter des virus, mais aussi de déceler des activités malveillantes, dangereuses ou criminelles qui ont lieu via internet.

## Comment fonctionne l'inspection approfondie des paquets ?

Quand vous envoyez ou recevez des informations par l'internet, elles subissent un processus très complexe et passent par de nombreux ordinateurs.

Les ordinateurs interconnectés par le World Wide Web fragmentent les informations que vous envoyez et recevez en petits morceaux appelés «paquets». Elles voyagent ainsi facilement à travers l'internet. Quand les paquets arrivent à leur destination, ils sont remis ensemble, comme les pièces d'un puzzle, pour recomposer le message. Chaque paquet porte une étiquette appelée «en-tête» ou « header » : elle décrit la nature du paquet, d'où il vient et où il va, la même chose que pour une lettre envoyée par la poste. Le paquet renferme le contenu du message, appelé «charge utile» ou « payload ».

Chaque paquet a plusieurs couches, qui contiennent chacune différentes informations au sujet du message. Ces couches s'emboîtent les unes dans les autres, un peu comme une poupée russe. Pour acheminer un message à destination, les fournisseurs de services internet doivent examiner quelques-uns des paquets qui le composent. Pour assurer la livraison du message, il leur suffit la plupart du temps de regarder l'en-tête (l'extérieur de l'enveloppe), sans considérer la charge utile (l'intérieur de l'enveloppe). Ceci s'appelle l'«inspection superficielle des paquets». En revanche, l'inspection approfondie des paquets (le DPI) inclut l'examen de tous les paquets d'un message et porte non seulement sur les en-têtes, mais aussi sur les contenus (charges utiles).



Les paquets sont inspectés au moyen d'algorithmes qui scrutent les messages à la recherche de certaines sortes de données. Les algorithmes sont des ensembles de calculs qui trient et analysent des données. Dans le DPI, un algorithme est programmé pour chercher certains «mots clés», de façon similaire à ce qui se passe quand vous effectuez une recherche dans un navigateur web. Les sortes de données visées dépendent de qui fait la recherche et de pourquoi elle est faite. Les mots clés utilisés peuvent se rapporter à des activités criminelles ou suspectes, à un nouveau virus informatique en circulation, ou encore à l'achat de tel ou tel produit.

L'inspection approfondie des paquets a lieu dans des «routeurs». Un routeur est un ordinateur qui dirige des messages vers les différents réseaux constituant l'internet. Tout l'équipement qui abrite la technologie qui effectue l'inspection approfondie des paquets est propriété de sociétés internet. Celles-ci peuvent contrôler le fonctionnement de l'internet aux niveaux local, régional, national et international. Les sociétés propriétaires des routeurs sont à l'origine de la technologie qui effectue l'inspection approfondie des paquets. Bien sûr, ces sociétés veulent utiliser cette technologie à leurs propres fins, mais elles peuvent aussi gagner de l'argent en vendant leur innovation à des tiers. D'autres sociétés, telles que des entreprises du secteur de la défense, ont aussi développé de la technologie DPI et veulent faire de même. Il existe maintenant un marché pour cette technologie.

## 5.2 Comment le DPI est-il utilisé ?

En Europe, on ne peut recourir au DPI que de façon très limitée. Sous les lois en vigueur, il peut intervenir pour «filtrer» le trafic internet à la recherche de virus et de logiciels malveillants. Il peut en outre aider les sociétés internet à gérer le trafic dans leurs réseaux. Mais le DPI est aussi capable d'analyser tout le contenu des communications en ligne. Utilisé de cette manière, il peut détecter des délits bien définis, tels que la diffusion de pornographie infantile. Mais cette utilisation est juridiquement controversée, parce qu'il n'existe aucune loi spécifique pour la réglementer. En effet, les lois européennes sur les technologies de communication ont été élaborées à un moment où le DPI n'existait pas.



Selon l'interprétation de la Cour européenne de justice et du Contrôleur européen de la protection des données, ces lois ne se rapportent qu'au «filtrage» limité des communications en ligne. D'autres lois seront nécessaires s'il faut réglementer en bonne et due forme l'usage plus détaillé du DPI.

Il s'ensuit que le DPI ne peut pas être utilisé légalement pour surveiller les communications en général, détecter le non-respect de copyrights, bloquer des contenus politiquement sensibles ou cibler la publicité, quand bien même la technologie est capable de faire toute cela. Même là où le DPI est autorisé, il ne peut pas être utilisé sans limite. Les lois européennes de protection des données et la Charte des droits fondamentaux de l'Union européenne protègent la confidentialité des communications. Le DPI contreviendrait aussi à la Convention européenne des droits de l'homme, parce qu'il implique une surveillance sans mandat, massive et non ciblée : il permet de lire chaque bit d'information échangé entre ordinateurs. La situation est très différente aux Etats-Unis, où le DPI n'est pas réglementé et où de nombreuses sociétés s'en servent pour cibler leur publicité. Si vous avez une adresse de courriel Gmail™ ou Yahoo™, il est presque certain que vos messages passent par les Etats-Unis et sont soumis au DPI. Il semble que le DPI ait été utilisé dans le cadre des programmes de surveillance de masse de l'Agence américaine de sécurité (NSA) et du Quartier-général des communications du gouvernement britannique (GCHQ) révélés pendant l'été 2013 (les programmes Upstream et Tempora).

La manière de détecter, limiter ou contrôler le DPI reste dans le flou. La réglementation essaie de rester en phase avec ce que la technologie est capable de faire. Il est très difficile de connaître l'ampleur du recours au DPI. Tout message envoyé peut voyager à travers le monde entier avant d'être reçu. Il peut avoir été soumis au DPI effectué par des fournisseurs de services internet ou des services de sécurité gouvernementaux dans un nombre indéfini de pays. Il est pratiquement impossible de le savoir. Le DPI fournit en outre des informations qui peuvent être partagées entre fournisseurs de services internet et gouvernements, et il est difficile de savoir ce qu'il advient des résultats des recherches. En l'absence de réglementation, nous sommes dans une situation de Far West, où les sociétés et les Etats peuvent exploiter cette zone grise de la législation.

Ce que nous pouvons dire est que dans le monde entier, de nombreuses institutions se servent du DPI. Des fournisseurs de services internet, des sociétés commerciales, la police et des agences nationales de sécurité y ont fait appel à diverses occasions. Mis à part les vastes activités de surveillance par des agences de sécurité américaines, révélées en 2013, peu d'utilisations du DPI ont été reportées : certaines sont commerciales et d'autres en relation avec la sécurité publique et nationale.

### 5.2.1 Utilisations commerciales

- > **Sécurité et gestion du réseau :** Les messages sont inspectés pour s'assurer qu'ils ne contiennent pas de virus, et le partage de fichiers de grande ampleur de personne à personne est souvent filtré.
- > **Publicité comportementale :** Des informations sur les préférences d'une personne en matière de produits sont collectées dans les messages. Ceci n'est pas permis en Europe, mais est bien accueilli par certains consommateurs aux Etats-Unis, où cette application du DPI est autorisée. Elle permet aux consommateurs de trouver des produits et services qui répondent à leurs besoins.
- > **Gestion des droits numériques :** Les messages sont inspectés pour déceler le partage illégal de fichiers et des violations du droit d'auteur.

### Polémique sur le DPI: Phorm et les données de consommateurs au Royaume-Uni

En 2008, une société américaine appelée Phorm a essayé de lancer un système au Royaume-Uni, en collaboration avec les fournisseurs de télécommunications British Telecom, Virgin Media and TalkTalk. Phorm utilisait le DPI pour intercepter les habitudes de navigation des usagers du web. Les données recueillies étaient ensuite analysées, avant d'être vendues à des annonceurs. Les fournisseurs de services avaient indiqué aux usagers que ces mesures étaient destinées à combattre la cybercriminalité, mais ils n'avaient pas révélé que les informations étaient utilisées pour de la publicité. British Telecom mena en secret des essais avec cette technologie et effectua plus de dix-huit millions d'interceptions. Des consommateurs britanniques ont appris la chose et protesté contre ce traitement de leurs données effectué sans leur consentement. Finalement, tous les fournisseurs de services ont abandonné la technologie de Phorm. Sur ce, la Commission européenne a engagé une action légale contre le gouvernement britannique qui avait permis l'utilisation de ce service. L'affaire a été classée en janvier 2012, après que le Royaume-Uni ait amendé sa législation. Celle-ci prévoit maintenant une sanction en cas d'interception illégale de communications.

### 5.2.2 Utilisations pour la sécurité publique et nationale

- > **Surveillance gouvernementale d'activités criminelles :** Encore que cela soit controversé sur le plan juridique, l'inspection approfondie des paquets est proposée comme outil d'investigation en relation avec des délits très spécifiques. Ceci concerne des délits:
  - > commis contre des systèmes informatiques ou en utilisant un ordinateur (p.ex. la diffusion de pornographie infantile) ;
  - > incluant le partage d'informations racistes ou des menaces racistes ;
  - > comprenant une incitation au terrorisme ou son organisation ;
  - > incluant le partage d'informations qui approuvent un génocide ou des crimes contre l'humanité.
- > **Censure:** On suppose que le DPI a été utilisé par des régimes répressifs partout dans le monde pour tromper des opposants politiques. Une société américaine du secteur de la défense, NARUS, une filiale de Boeing, a vendu de la technologie DPI à la Libye, qui l'a utilisée pour réprimer la dissidence pendant le printemps arabe. Par contre, toujours dans le sillage du printemps arabe, le Royaume-Uni a limité la vente de technologie DPI à l'Egypte, au Bahreïn et à la Libye, en révoquant des licences d'exportation. Bien qu'on ne soit pas au clair sur le fournisseur de la technologie utilisée, l'Iran se sert du DPI non seulement pour connaître et censurer les informations auxquelles les citoyens ont accès, mais aussi pour modifier des contenus en ligne à des fins de désinformation. La Chine utilise le DPI de façon similaire. La question se pose de savoir si la censure de l'internet est pratiquée aussi en Europe.

### 5.3 Améliorations de la sécurité

L'inspection approfondie des paquets peut améliorer la sécurité de l'information et la lutte contre la criminalité en identifiant et bloquant des messages dangereux, nuisibles ou criminels, décrits au paragraphe 5.2.2 ci-dessus.

Bien que le DPI ne puisse pas prévenir les délits graves auxquels ces messages se rapportent, il permet de les détecter et peut fournir des indices pendant une enquête. Il peut aussi prévenir la propagation de virus informatiques et d'autres formes de cybercriminalité.

## 5.4 Enjeux

L'inspection approfondie des paquets soulève les graves problèmes suivants :

1. Rien n'échappe au DPI.
  - > Il peut analyser tous les messages qui circulent sur un réseau et les données sensibles qu'ils sont susceptibles de contenir. Cela signifie que soumises au DPI, les communications électroniques ne sont plus privées.
  - > Le fait de savoir que les communications ne sont plus privées peut avoir un grave effet d'intimidation sur les gens. Ils auront peur de communiquer ouvertement et de s'exprimer librement.
  - > Vu l'énorme puissance du DPI, il faut que son utilisation soit strictement réglementée.
2. Les moyens techniques évoluent plus vite que la réglementation.
  - > Il n'existe pas de règles juridiques claires indiquant à quelles fins le DPI peut et ne peut pas être utilisé.
  - > Dans la pratique, l'utilisation du DPI dépend de l'éthique de celui qui s'en
3. Il est difficile de localiser avec précision où le DPI est utilisé et par qui.
  - > Il faudrait que les dispositions légales soient les mêmes partout dans le monde. Dans le monde entier, des responsables de la protection des données demandent depuis quelque temps une norme minimale internationale en matière de vie privée.
  - > Un organisme de réglementation du DPI devrait être véritablement international et disposer de suffisamment de pouvoir pour sanctionner les infractions.
4. L'efficacité du DPI est incertaine.
  - > Etant donné que des ordinateurs détectent des messages qui ne sont que potentiellement problématiques, une interprétation incorrecte peut conduire à suspecter un innocent.
  - > Certains experts mettent en question l'efficacité du DPI à trouver des contenus illégaux.



**«De nombreuses entreprises qui utilisent le DPI pour analyser des données ayant trait à des citoyens et citoyennes européens se trouvent hors d'Europe. C'est la raison pour laquelle on ne peut pas leur dire de ne pas le faire.»**

**Eva Schlehahn, membre de l'Autorité indépendante de protection des données du Land allemand de Schleswig-Holstein**



## 6 La géolocalisation des smartphones

**Quand Aisha a allumé son smartphone, elle a remarqué que sa localisation avait changé sur l'écran d'accueil. Elle était sûre qu'il devait y avoir derrière cela une explication toute simple. En effet, tous les téléphones mobiles ont besoin de savoir où ils se trouvent pour fonctionner. Mais les smartphones répondent à cette exigence à un niveau entièrement nouveau.**

Le téléphone mobile intelligent a presque éclipsé le couteau suisse en tant qu'outil et jouet parfait tout en un. Il existe en gros cinq milliards de raccordements à la téléphonie mobile dans le monde. En Europe, on compte près de 1.3 téléphones mobiles par personne. C'est un nombre énorme si l'on considère que ces appareils au format de poche n'étaient pas disponibles jusqu'au début des années 1990.

### 6.1 Pourquoi a-t-on développé la géolocalisation des smartphones ?

Les smartphones sont relativement récents. Leur énorme popularité tient à ce qu'ils sont capables de faire de nombreuses choses différentes tout en étant aussi un téléphone portable normal. En fait, les smartphones sont plutôt de petits ordinateurs de poche permettant accessoirement de téléphoner. Comme un ordinateur de bureau ou un laptop, chaque type de smartphone possède son système d'exploitation, nécessaire pour échanger des courriels et naviguer sur le web. Les smartphones peuvent exécuter des applications offrant des services tels que jeux, cartes topographiques et dernières nouvelles en ligne. Ils comprennent également des appareils photo numériques et des caméras vidéo, des lecteurs multimédia et des écrans tactiles plus grands et en couleurs.

L'histoire des téléphones mobiles remonte à la Seconde Guerre mondiale. A la base, un téléphone mobile est pour l'essentiel une radio sans fil qui sert à envoyer et recevoir des messages. Les premières de ces « radios », les « walkie talkies », ont été introduites pour permettre aux soldats de rester en contact sur le front. Les premiers combinés portatifs sont apparus dans les années 1970 et 1980, grâce aux progrès des microprocesseurs. Le

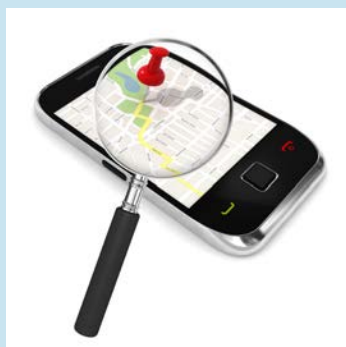
premier téléphone mobile avait la taille et le poids d'une brique et sa batterie fournissait seulement vingt minutes de courant. Que les temps ont changé ! A partir des années 1980, le développement d'un réseau d'antennes relais a amélioré les signaux téléphoniques aussi bien localement qu'à grande distance. Vous vous souvenez peut-être : c'est au milieu des années 1990 que les antennes ont commencé à se multiplier. L'emplacement de ces mâts jugés inesthétiques et les problèmes pour la santé d'une augmentation des niveaux de rayonnement ont alimenté de nombreuses discussions dans le public.



Les antennes relais jouent un rôle très important pour la localisation des téléphones mobiles. Chacune d'elles couvre une zone géographique bien définie. Pour se connecter au réseau, faire des appels et envoyer des textes, les téléphones mobiles s'enregistrent auprès de l'antenne la plus proche. L'antenne à laquelle un téléphone est connecté enregistre toujours la localisation de l'appareil. Si la personne qui se sert du téléphone se déplace et entre dans le rayon d'une autre antenne, celle-ci prend à son tour l'appareil en charge, à la place de la précédente. Le déplacement d'une personne portant sur elle un téléphone peut ainsi être suivi par les fournisseurs de télécommunications. Les réglementations en vigueur dans l'Union européenne exigent que les opérateurs conservent ces données pendant au moins six mois et jusqu'à deux ans. Il y a encore d'autres moyens de localiser les smartphones. L'utilisateur peut configurer son téléphone de manière à ce que l'appareil établisse sa position en se référant à des satellites d'un système mondial de positionnement ou en se connectant à des réseaux sans fil.

Ceci a conduit à une énorme croissance de l'offre de «services géolocalisés» pour les smartphones. Ils sont généralement disponibles comme applications (des «apps») qui peuvent être installées sur le téléphone. Une app est un logiciel qui exécute une fonction ou un service spécifique. Les apps géolocalisées permettent à un utilisateur de trouver des informations sur des restaurants ou

des magasins dans le voisinage, ou de savoir lesquels de ses amis se trouvent à proximité. Des jeux géolocalisés sont aussi disponibles. Les services géolocalisés connaîtront probablement une utilisation croissante dans les années à venir.



## Comment fonctionne la géolocalisation des smartphones ?

La géolocalisation est possible aussi bien pour les téléphones portables traditionnels que pour les modèles «intelligents» (smartphones). Il y a trois manières d'effectuer cette localisation : par le biais des antennes relais, de systèmes mondiaux de positionnement ou de réseaux sans fil. La première de ces méthodes s'applique à tous les téléphones mobiles, les deux autres seulement aux smartphones.

**Antennes relais:** Pour envoyer et recevoir des appels, des textes et des courriels par le réseau mobile, les téléphones mobiles, quel que soit leur type, s'enregistrent auprès de l'antenne relais la plus proche. Chaque téléphone contient un numéro de référence unique, qui associe l'appareil à un compte auprès de la société de téléphonie mobile, et donc aussi à l'utilisateur. Cette information sert aussi à établir la facture de téléphone. Si des services de sécurité ou les forces de l'ordre essaient de suivre les déplacements d'une personne à un moment donné, ils peuvent requérir des données d'antennes relais auprès des sociétés de téléphonie mobile. Les enregistrements effectués par ces antennes indiquent si le téléphone de la personne en question s'est trouvé dans le rayon de telle ou telle antenne. Si cela est fait pour toutes les antennes – comme exigé dans l'UE – il est possible de retracer les localisations du téléphone et de repérer les déplacements de son propriétaire.

**GPS:** Les smartphones contiennent un logiciel de cartographie et des applications qui fonctionnent en se référant à des données GPS. Quand la fonction GPS d'un smartphone est activée, le téléphone détermine sa position sur la planète en calculant à quelle distance il se trouve des satellites GPS les plus proches. Quand la fonction est désactivée, le téléphone ne peut plus se localiser en recourant au GPS. Des fournisseurs d'apps collectent ces données de localisation et certains d'entre eux les vendent à des fins de marketing. Si les services de sécurité ou les forces de l'ordre suivent les déplacements d'une personne, ils peuvent requérir des données GPS auprès des sociétés de téléphonie.

**Réseaux sans fil (wifi):** Les smartphones peuvent se connecter à des réseaux sans fil en service dans une zone donnée. Par cette connexion, le téléphone est localisé dans les limites d'un réseau sans fil. Dans ce cas aussi, une fois cette fonction désactivée, le téléphone ne peut plus être localisé de cette manière. Un point d'accès wifi a généralement une portée d'une vingtaine de mètres à l'intérieur d'un bâtiment, mais plus grande à l'extérieur.

D'autres appareils personnels mobiles, tels que tablets, iPads et notebooks, peuvent être localisés de la même manière.



Les services géolocalisés offrent de nombreux avantages aux utilisateurs de smartphones. Cependant, des défenseurs des droits à la vie privée s'inquiètent du niveau d'information que peut procurer la géolocalisation des smartphones. Par exemple, lorsque l'homme politique allemand Malte Spitz, membre des Verts, a essayé d'obtenir les enregistrements de six mois de données de localisation de son téléphone mobile, il lui a fallu poursuivre en justice la société de téléphonie pour obtenir ces informations. A première vue, les données qu'il avait enfin reçues se présentaient comme une suite de chiffres et de lettres apparemment dénuée de sens. Mais Malte les fit examiner par un statisticien et y découvrit alors un reflet détaillé de sa vie. En collaboration avec le journal «Die Zeit», Malte produisit un film d'animation décrivant exactement où il avait été au cours de cette demi-année. Malte s'est alarmé du nombre de détails qui pouvaient être révélés à son sujet, notamment lorsque les données relatives à la localisation étaient combinées avec des informations provenant de médias sociaux tels que Twitter ou Facebook.

Dans une affaire traitée récemment par la Cour suprême des Etats-Unis, *United States v. Jones*, le juge a constaté que des données GPS mettent en évidence des déplacements relevant indiscutablement de la sphère privée, par exemple pour aller chez le psychiatre ou le chirurgien esthétique, dans une clinique d'avortement, un centre de traitement du SIDA ou un club de strip-tease, chez un avocat de la défense, dans un motel, à une réunion syndicale, à la mosquée, la synagogue ou l'église, dans un bar gay, etc.

## 6.2 Comment la géolocalisation des smartphones est-elle utilisée ?

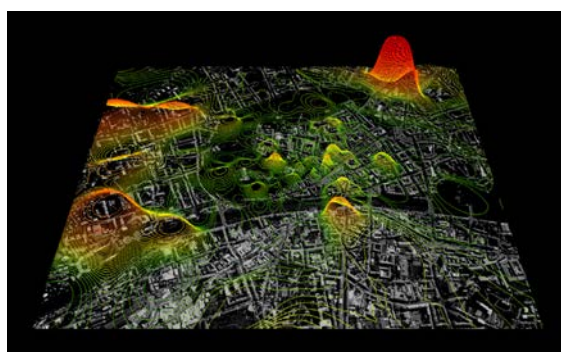
La géolocalisation des smartphones est utilisée aussi bien à des fins commerciales que de sécurité.

### 6.2.1 Utilisations commerciales

- > **Administration des factures de téléphone :** Les sociétés de téléphonie mobile ont besoin de données de localisation ainsi que du numéro d'identification du téléphone pour facturer les communications.

- > **Marketing ciblé :** Des éditeurs de logiciels qui produisent des apps, tels que Twitter, Angry Birds ou FourSquare, recueillent des données de localisation et d'autres informations de contact par le biais de téléphones et les vendent à des annonceurs. A l'aide de ces données, les annonceurs élaborent ensuite leur publicité pour des produits vendus en fonction du lieu et du type de consommateurs. Angry Birds, par exemple, a été téléchargé un milliard de fois dans le monde. Des usagers ont découvert avec surprise que son développeur finlandais, Rovio Entertainment Ltd, collectait et vendait systématiquement les données de localisation des joueurs. Cinquante pour cent des apps recueillent des données même quand elles n'en ont pas besoin pour fonctionner.

- > **Planification urbaine :** Des données de localisation peuvent être employées pour cartographier l'utilisation d'espaces urbains. Comme ceux-ci comprennent davantage d'antennes relais que les zones rurales, les téléphones peuvent y être localisés de façon beaucoup plus précise. Cette image plutôt fantomatique est une carte de l'utilisation des téléphones mobiles à Graz, en Autriche. Des chercheurs du Massachusetts Institute of Technology ont localisé anonymement ces appareils pour construire une image montrant comment les gens se déplacent dans la ville. Leur but est d'informer les urbanistes et les planificateurs en transports sur l'utilisation de la ville.



## 6.2.2 Utilisations pour la sécurité publique et nationale

- > Recherche de personnes disparues ou blessées : Aux Etats-Unis et au Canada, un service appelé E-911 impose légalement l'utilisation du GPS sur tous les téléphones mobiles afin de pouvoir les localiser (ainsi que leurs utilisateurs) en cas d'urgence. En Europe, environ 180 millions d'appels d'urgence sont lancés chaque année. Soixante à septante pour cent proviennent de téléphones mobiles. Ceux-ci révèlent leurs données de localisation au 112, le numéro d'urgence valable dans toute l'Europe (y compris en Suisse, où il est redirigé vers Police-Secours). A la différence des Américains et des Canadiens, les Européens ne sont pas tenus de laisser en marche en permanence le GPS de leur téléphone.
- > Suivi des déplacements de suspects : Les services de sécurité et les forces de l'ordre peuvent accéder à des données de localisation en soumettant une demande de données à des sociétés de téléphonie mobile. Actuellement, toute requête de ce genre est régie en Europe par la loi. Lorsqu'elles reçoivent une telle demande, les sociétés sont tenues de remettre aux services de sécurité toutes les données relatives à un suspect. Pour suivre la trace d'un téléphone, les services de sécurité disposent encore d'autres méthodes, qui permettent de cibler des individus spécifiques.
- > Localisation de membres d'une famille : Des particuliers peuvent aussi bénéficier de services géolocalisés. Par exemple, de nombreux parents font usage de produits qui leur permettent, grâce à la localisation de téléphones mobiles, de savoir en permanence où leurs enfants se trouvent.

### Controverse sur la géolocalisation des smartphones

A la suite du mouvement «Occupy» à New York, Twitter a été sommé de fournir des données de localisation au gouvernement américain pour lui permettre d'identifier les protestataires. Récemment, Twitter a lancé un nouveau service appelé «Please Don't Stalk Me» (s.v.p. ne me traquez pas). Il permet à ses utilisateurs de travestir les données de localisation attachées à leurs tweets. Avec cette app, les utilisateurs définissent un lieu quelconque sur la planète par le biais de Google Maps et incorporent cette donnée truquée à leurs tweets. D'autres apps, telles que «My Fake Location», «Fake GPS Location» et «GPS Cheat» font la même chose.

## 6.3 Améliorations de la sécurité

La géolocalisation des smartphones améliore la sécurité de plusieurs manières :

1. Elle permet de trouver et d'aider des personnes en danger.
2. Elle permet à des adultes vulnérables et à des enfants d'être suivis par leurs familles.
3. La police et les forces de l'ordre peuvent se servir de données de localisation pour constater la présence d'individus sur le lieu d'un délit ou écarter des soupçons à leur rencontre.



## 6.4 Enjeux

La géolocalisation des smartphones soulève les questions suivantes ayant trait à la vie privée, à la réglementation et aux droits de l'homme :

1. Les utilisateurs n'ont pas l'entier contrôle des informations révélées par leurs smartphones. Ceci est un point particulièrement délicat pour des utilisateurs vulnérables, tels que des témoins sous protection qui ne souhaiteraient pas faire connaître leur données de localisation, mais aimeraient bénéficier néanmoins des avantages d'un téléphone mobile. Certains téléphones, tels que les iPhones d'Apple, enregistrent automatiquement ces données, sans possibilité de désactiver cette fonction.
2. Certaines apps collectent des données de localisation même quand elles n'en ont pas besoin pour fonctionner. A défaut d'une forte pression de la part du public, il y a peu de chances que des sociétés donnent aux consommateurs un meilleur contrôle de leurs données de localisation.
3. Nombre de développeurs d'apps se trouvent hors d'Europe et ne sont donc pas soumis aux lois de protection des données en vigueur sur ce continent. C'est pourquoi l'UE peut difficilement exiger que ces apps respectent la vie privée. Toutefois, un récent amendement de la directive «Vie privée et communications électroniques» souligne que les utilisateurs doivent avoir la possibilité de donner leur consentement au traitement de données provenant d'apps de leurs smartphones, quel que soit le lieu où le fournisseur de l'app est basé dans le monde.
4. De façon similaire au DPI, dans des pays où les opérateurs de téléphonie mobile entretiennent des relations étroites avec le gouvernement, les informations peuvent être échangées de manière à donner à l'Etat accès aux données de localisation de tous les citoyens.
5. Le fait que des données de localisation aient été utilisées pour identifier des protestataires peut avoir un effet d'intimidation et faire hésiter des personnes à contester et exercer leurs droits démocratiques.



**«La géolocalisation de smartphones donne de nouvelles possibilités aux utilisateurs tout en les surveillant. Elle**

**fournit de nombreux services et peut renforcer les relations sociales ... mais il n'est pas toujours évident ni facile de manipuler les préférences de partage de données de localisation.»**

Gus Hosein, Privacy International



# 7 La vidéosurveillance intelligente

Plus haut dans cette brochure, nous avons relaté qu'Aisha, sur la route de l'aéroport, s'est demandé comment fonctionnaient les caméras utilisées pour encaisser son péage routier. Il s'agissait de caméras de lecture automatique des plaques d'immatriculation ou caméras LAPI. Les caméras LAPI sont un exemple d'une nouvelle technologie de sécurité appelée vidéosurveillance intelligente.

Le principe d'un système de vidéosurveillance est familier à la plupart des Européens. Un système «traditionnel» de vidéosurveillance comprend des caméras mises en place sur le mobilier urbain dans des espaces publics ou dans des magasins. Les caméras sont connectées à une salle de contrôle par une liaison de télécommunications. Dans la salle de contrôle, des rangées d'écrans permettent à des opérateurs formés à cet effet de voir les images captées par les caméras. Les images sont enregistrées, stockées, puis effacées après un certain délai. Le système est «fermé» : les images ne sont pas diffusées ailleurs que dans la salle de contrôle. Si les opérateurs remarquent quelque chose de suspect, ils peuvent contacter le gardien ou la police par téléphone ou par radio pour les faire intervenir.



## 7.1 Pourquoi a-t-on développé la vidéosurveillance intelligente ?

A l'origine, la vidéosurveillance a été développée pour observer le lancement de missiles pendant la Seconde Guerre mondiale et pour commander à distance des processus industriels dangereux. Elle a été commercialisée comme technologie de sécurité la première fois aux Etats-Unis dans les années 1950. La police l'a adoptée aux Etats-Unis et en Grande-Bretagne au cours des années 1960. Le recours à la vidéosurveillance a connu une progression constante à travers l'Europe pendant les années 1990 (le Royaume-Uni venant en tête, suivi de près par la France et les Pays-Bas) et il a toujours été au centre de l'attention des médias. En 2013, la vidéosurveillance a joué un rôle clé à Boston pour identifier les auteurs de l'attentat du marathon.

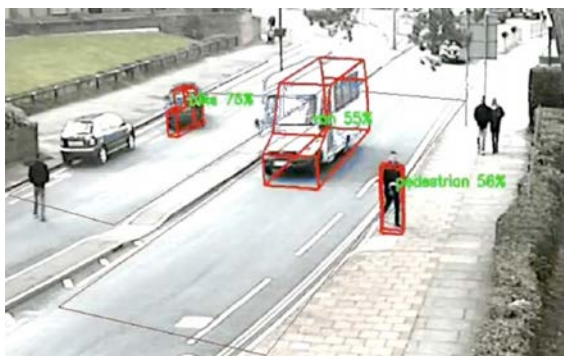
La vidéosurveillance intelligente a été développée pour remédier à un problème auquel la vidéosurveillance était confrontée depuis ses débuts, à savoir le fait qu'il y a trop de caméras et trop peu d'yeux pour suivre ce qui se passe. A la différence de la vidéosurveillance «traditionnelle», un système de vidéosurveillance intelligente utilise un réseau de caméras numériques connectées à des dispositifs capables d'analyser les images qu'elles produisent. Un logiciel examine ce qui se passe sur l'image. S'il y a quelque chose d'inhabituel, une alarme sonne et attire l'attention de l'opérateur sur l'image en question. L'alarme est enregistrée. Les images qui lui sont associées sont stockées dans un ordinateur et peuvent être retrouvées et partagées facilement.

La vidéosurveillance intelligente peut faire plusieurs choses. Elle est utilisée pour :

- > identifier des objets dans une image, par exemple un véhicule en lisant sa plaque minéralogique et en la comparant avec les informations stockées dans une base de données ;
- > reconnaître le visage d'une personne, quand elle apparaît devant un arrière-plan uni et dépouillé. Pour identifier la personne, cette image est comparée avec les photos conservées dans une base de données d'individus connus ;
- > déceler un bagage non surveillé (seulement s'il est laissé dans un espace vide).

La vidéosurveillance intelligente n'est pas fiable dans toutes les situations, mais des logiciels sont en développement pour :

- > identifier des personnes dans une foule en repérant leurs vêtements ;
- > détecter un comportement suspect ou inhabituel dans la scène observée, le vagabondage par exemple. Les comportements dans les images sont comparés à des types de comportements connus, stockés dans une base de données.



Cependant les systèmes de vidéosurveillance intelligente ne sont pas tous pareils. La «perspicacité» d'un système dépend de la qualité de l'analyse de l'image par le logiciel et de ce qui se passe avec l'image une fois celle-ci partagée. Les systèmes sont installés

dans différents buts, aussi un système de vidéosurveillance intelligente n'est pas forcément capable d'effectuer toutes les tâches décrites plus haut. Certaines de ces tâches peuvent ne pas être utiles au propriétaire d'un système.

## 7.2 Comment la vidéo-surveillance intelligente est-elle utilisée ?

Les systèmes de vidéosurveillance intelligente sont des produits commerciaux vendus par des sociétés de technologies de sécurité et de défense. De nombreux systèmes sont déjà disponibles. Actuellement, les principaux utilisateurs institutionnels de la vidéo-surveillance intelligente sont les responsables d'infrastructures de transport, telles qu'auto-roues, aéroports, installations portuaires ou chemins de fer, les autorités locales et la police.

A Budapest, à la fin des années 2012, la police a commencé à utiliser des caméras de vidéo-surveillance intelligente pour observer les couloirs réservés aux autobus. Elle peut se servir légalement des images tant que les passagers ne sont pas filmés et que le public est pleinement informé.

Des caméras de reconnaissance faciale sont en place depuis 2003 à l'aéroport de Zurich. A

### Comment fonctionne la vidéo-surveillance intelligente ?

Grâce à des «algorithmes intelligents», un ordinateur connecté à un système de vidéosurveillance intelligente apprend à reconnaître des types spécifiques de comportements publics, connus comme «événements déclencheurs» - par exemple une personne qui tient un revolver ou qui reste immobile dans une foule en mouvement. Un algorithme est un ensemble de calculs qui trie les données contenues dans les images numériques.

Un algorithme est dit «intelligent» s'il apprend ce qu'il doit chercher au fur et à mesure qu'il analyse des données.

Les algorithmes intelligents utilisés dans des systèmes de vidéosurveillance sont conçus de manière à reproduire le fonctionnement de l'œil et du cerveau humains. Le logiciel fragmente une image en très petits éléments, appelés «pixels». Vous connaissez le terme de pixel si vous avez une caméra numérique ou un smartphone. Si une caméra numérique a 8 mégapixels, chaque image qu'elle capte comprend 8 millions de pixels.

L'algorithme est alors capable de calculer le degré de mouvement de chaque pixel de l'image. Ceci permet au logiciel de déceler les zones actives de chaque scène enregistrée par les caméras, à partir de quoi il apprend à reconnaître des types de mouvements dans une image. Puis le système identifie et classe des événements en fonction des types de mouvements qu'il connaît déjà. Par exemple, le logiciel fait la distinction entre des spectateurs passifs et des fans qui sautent de joie pendant un match de football.

l'époque, c'était la première fois que la reconnaissance faciale était utilisée dans le contexte de contrôles aux frontières. Ce système est maintenant installé de façon permanente.

L'Union européenne a financé seize projets distincts de développement d'algorithmes et de fonctions de systèmes de vidéosurveillance intelligente. Des applications complexes, telles que la détection de comportements suspects ou de visages dans la foule, sont actuellement encore en développement et en phase d'optimisation. Leur utilisation est encore peu répandue, et tout le temps de nouveaux systèmes sont testés. Par exemple, les autorités de transport de Rome, Londres, Paris, Bruxelles, Milan et Prague ont participé récemment à des essais avec un système de surveillance des piétons qui recourt à la vidéosurveillance intelligente. Il alerte les opérateurs en cas de paquets suspects, de mouvements anormaux de passagers et de comportements inhabituels. Il n'est pas en usage opérationnel, mais est encore en phase de test au moment où nous écrivons ce chapitre.

L'application la plus répandue de la vidéosurveillance intelligente est peut-être la lecture automatique des plaques d'immatriculation (LAPI). L'image numérique du numéro de plaque donne une information qui peut être comparée avec les bases de données officielles des détenteurs de véhicules, les banques de données des assurances et celles de la police. Le détenteur du véhicule et l'adresse à laquelle il est enregistré sont facilement identifiés, et la caméra LAPI localise avec précision un individu donné dans l'espace et le temps. Ce système peut servir à identifier des véhicules volés, ou conduits sans que l'impôt ait été acquitté ou sans assurance, ou en infraction d'excès de vitesse.



Une question est de savoir si ces différents types de délits justifient le même niveau de surveillance. La vidéosurveillance intelligente doit-elle être utilisée pour tous les types de délits ou employée uniquement pour les infractions pénales les plus dangereuses ? Les opinions à ce sujet varient à travers l'Europe. En Allemagne par exemple, la cour constitutionnelle a limité en 2008 le recours à la LAPI par la police pour des raisons de confidentialité. La cour a souligné que les forces de police ne devaient conserver des données numériques recueillies par des caméras LAPI que si leur vérification dans des bases de données était immédiate et suivie d'effets. La LAPI est également utilisée pour le prélèvement des péages routiers, mais ceci aussi a suscité des critiques, car il existe d'autres moyens moins intrusifs de percevoir cette taxe. En Grande-Bretagne, la LAPI a par exemple été utilisée pour le prélèvement des péages routiers à Londres, mais elle est maintenant intégrée aux stratégies tant nationales que locales de maintien de l'ordre. Depuis 2010, cinq mille caméras LAPI ont été installées au Royaume-Uni, où le centre de données national de la police reçoit entre 10 et 14 millions d'enregistrements LAPI par jour.

## La controverse au sujet de la vidéosurveillance intelligente : la LAPI à Birmingham, au Royaume-Uni

En 2011, la police britannique a dû enlever des caméras LAPI de trois quartiers à forte population musulmane de la ville de Birmingham. Ces caméras étaient financées dans le cadre d'un programme anti-terroriste, le «Project Champion», mais avaient été justifiées auprès du public par des raisons de sécurité. Des responsables locaux et des membres du parlement communal se sont fermement opposés à l'utilisation de ces caméras et cette affaire a nui aux relations entre communautés. Deux cents caméras étaient installées, mais aucune ne fut mise en service. Soixante-quatre de ces caméras étaient cachées et avaient été installées sans consulter la population. Les caméras furent soit détruites, soit utilisées par d'autres forces de police britanniques. L'échec de ce projet et la perte des caméras ont coûté 300'000 £ (environ 450'000 francs suisses) à la police.



## 7.3 Améliorations de la sécurité

La vidéosurveillance intelligente peut améliorer la sécurité des manières suivantes.

1. Les problèmes de sécurité sont plus faciles à déceler dès qu'ils se présentent :
  - > Le système remarque ce qui est inhabituel et alerte l'opérateur de la vidéosurveillance en actionnant une alarme. L'opérateur peut ainsi plus facilement interpréter des images.
  - > L'alarme aide l'opérateur à prendre des décisions plus rapides et plus efficaces quant à la nécessité ou non d'intervenir pour maîtriser un problème de sécurité.
  - > Les algorithmes du système pouvant traiter de très grands volumes d'informations, ils parviennent quelquefois à repérer des détails susceptibles d'échapper à un opérateur.
2. La crainte diminue tant à l'égard de la criminalité que du caractère intrusif de la vidéosurveillance :
  - > Si la technologie de sécurité fonctionne de façon efficace, les gens sont rassurés, parce qu'ils savent que quelque chose d'inhabituel autour d'eux sera repéré rapidement par un système de vidéosurveillance intelligente.
  - > Les caméras de vidéosurveillance intelligente prennent des images beaucoup plus détaillées que les caméras de vidéosurveillance traditionnelle. Cela signifie qu'un espace donné peut être contrôlé avec moins de caméras. Il s'ensuit que la vidéosurveillance intelligente peut être perçue comme moins intrusive du fait que moins de caméras sont présentes.
  - > La protection de la vie privée peut être améliorée en masquant des zones sensibles sur les images, par exemple l'intérieur de propriétés privées, pour que l'opérateur ne les voie pas.

## 7.4 Enjeux

La vidéosurveillance intelligente a plusieurs inconvénients qu'il faut prendre en considération.

1. Les algorithmes utilisés actuellement en vidéosurveillance intelligente présentent un certain nombre de problèmes et de points faibles. Ceux-ci peuvent donner lieu à de «fausses alarmes» qui signalent à tort un incident de sécurité. Une conséquence possible est qu'un innocent soit confondu avec un suspect. Les points faibles actuels sont les suivants :
  - > Seulement certains types d'objets, tels que la plaque minéralogique d'une voiture ou un bagage laissé sans surveillance dans un espace vide, peuvent être repérés de manière fiable.
  - > Les caméras sont peu efficaces pour identifier ce qui se passe dans une foule.
  - > Les délits effectués de façon discrète, tels que le vol à la tire ou à l'étalage, sont difficiles à déceler.
  - > Les algorithmes sont sujets à des biais, parce qu'ils sont programmés par des êtres humains pour identifier ce que ceux-ci considèrent comme «anormal». D'où le danger que des systèmes soient délibérément ou accidentellement programmés pour cibler des minorités de façon discriminatoire.
  - > A l'avenir, si un délinquant potentiel sait que la vidéosurveillance intelligente est utilisée, il pourra éviter d'être localisé simplement en changeant de vêtements, étant donné que les algorithmes fonctionnent en reconnaissant les habits portés par des suspects.
  - > La proportion élevée de fausses alarmes envoyées aux opérateurs peut amener ceux-ci à perdre confiance dans le système et à ignorer ce qu'il leur signale.

2. Les caméras de vidéosurveillance intelligente sont à la fois plus performantes et plus petites :
  - > Elles captent davantage d'informations. Leur atteinte à la vie privée est ainsi potentiellement plus importante et les activités de personnes innocentes sont plus susceptibles d'être observées et analysées.
  - > Les caméras sont moins faciles à repérer. Il est donc plus difficile pour les gens de savoir s'ils sont sous vidéosurveillance, et moins aisé pour eux de la contester ou de l'éviter.
  - > La liberté d'expression de même que la dignité de la personne peuvent être affectées si le comportement des gens dans l'espace public est suivi de près par l'action conjuguée de logiciels et du personnel de surveillance.
3. Des êtres humains sont encore nécessaires pour exploiter le système :
  - > Quelqu'un doit interpréter les images et confirmer si l'alerte est bien réelle. S'il est possible au système de déceler des comportements inhabituels, il n'explique pas, en revanche, le pourquoi de ces comportements.
  - > Les institutions doivent être très étroitement réglementées quant aux types de recherches à effectuer et aux garanties contre l'usage abusif de données.



**«Les raisons qui motivent l'installation d'un système de vidéosurveillance intelligente doivent être transparentes. Les gens devraient être habilités à contacter l'exploitant du système pour lui demander à quoi il sert. Les gens doivent être convaincus que la caméra est là pour de bonnes raisons et ils doivent être confiants quant à son utilisation».**

**Chris Tomlinson, responsable de planification en sécurité**





## 8 La technologie est-elle la seule réponse ?

Vous vous demandez peut-être si les technologies de surveillance sont la seule solution aux problèmes de sécurité. Il semble parfois que la sécurité se résume à localiser et identifier des suspects au sein de la population. Or cela n'est qu'un aspect de la question.

Les priorités européennes en matière de sécurité, dont nous avons parlé plus haut, semblent suggérer que la sécurité joue un rôle important dans tous les domaines de la vie. Elles concernent les aspects de la sécurité «classique» tels que la criminalité et le terrorisme. Comme nous l'avons vu dans les pages précédentes, il est possible d'utiliser de nouvelles technologies de sécurité pour chercher des personnes impliquées dans de telles activités. Mais des phénomènes sous-jacents peuvent être à l'origine de ces problèmes de sécurité, par exemple la pauvreté, des conflits nationaux ou internationaux, ou des clivages politiques et religieux. Les technologies de sécurité ne sont pas en mesure de s'attaquer à ces causes profondes.

Les priorités européennes de sécurité considèrent aussi les crises et les catastrophes comme des problèmes de sécurité. Ces calamités peuvent inclure des pénuries de nourriture ou d'eau, des crises financières, la propagation de maladies, ou des catastrophes naturelles qui sont autant de défis pour la sécurité humaine. Encore une fois, les technologies de surveillance sont peu efficaces pour faire face à ces problèmes de sécurité à long terme et bien plus complexes.

Ainsi, bien que des technologies de sécurité soient utilisées pour trouver des criminels et des terroristes et anticiper leurs prochains déplacements, d'autres solutions entrent aussi en ligne de compte. Nous en énumérons quelques-unes ci-dessous. Il se peut que vous ayez vos propres idées sur la manière d'améliorer la sécurité. Ou vous pensez peut-être que les objectifs de sécurité de l'Europe devraient se distancer de la criminalité et du terrorisme et se centrer sur d'autres priorités.

### 8.1 Solutions locales

- > Promouvoir un environnement construit plus sûr, grâce à un bon éclairage des rues, des téléphones publics pour appels d'urgence et une plus forte présence de la police.
- > Améliorer les relations entre la population locale et la police, en prenant des mesures de prévention de la criminalité au niveau de la collectivité.
- > Laisser des groupes confessionnels et d'autres associations locales gérer des problèmes locaux, afin d'accroître la confiance sociale.
- > Veiller à la transparence et à la fiabilité des autorités et de la police.
- > Avoir assez d'emplois et de possibilités de formation et d'encadrement pour les individus les plus susceptibles d'être associés à des actes criminels

### 8.2 Solutions nationales ou internationales

- > Promouvoir des systèmes mondiaux de commerce équitable, d'aide et d'allègement de la dette.
- > Améliorer les infrastructures et ressources d'intervention en cas de catastrophes.
- > Améliorer les infrastructures de communication et d'information, ainsi que d'approvisionnement en eau et en denrées alimentaires, dans les régions du monde qui en ont besoin.
- > Utiliser de façon plus efficace les ressources énergétiques durables et de substitution.
- > Résoudre des problèmes d'inégalité et de discrimination.



## 9 A vous maintenant !

Nous espérons que vous ne vous sentez pas submergé par ce flot d'informations ! La bonne nouvelle est que vous êtes arrivé maintenant à la fin de cette brochure et que vous pouvez prendre un peu de temps pour penser et réfléchir aux questions que nous avons soulevées.

Nous avons présenté les technologies de sécurité qui seront discutées lors des forums de discussion SurPRISE. Nous avons expliqué comment elles fonctionnent, comment elles sont utilisées, les améliorations qu'elles offrent en termes de sécurité et les problèmes qu'elles posent. Nous avons également décrit le contexte dans lequel ces technologies ont été développées : une Europe qui est très préoccupée par la sécurité et où celle-ci fait partie de la vie de tous les jours. Le rapport entre surveillance et vie privée suscite des questions importantes en raison de la quantité de données personnelles utilisée aujourd'hui dans le contexte de la sécurité. Enfin, nous avons examiné s'il existe d'autres solutions, des approches non technologiques pour assurer la sécurité dans la société.

A vous maintenant de vous faire une opinion sur ces questions. Si ces technologies étaient mises en œuvre systématiquement à des fins de sécurité, dans quelle mesure seraient-elles acceptables ? Il vous semble peut-être que chacune d'elles est efficace à sa manière pour accroître la sécurité et pourrait réduire la criminalité. Mais il se peut aussi que d'autres solutions, non technologiques, vous paraissent meilleures. Vous pensez peut-être qu'il faudrait recourir à des méthodes plus traditionnelles, mises en œuvre par du personnel de sécurité bien formé ou par la police, plutôt qu'à une surveillance basée sur la collecte d'informations à grande échelle.

Ou vous vous dites peut-être que la sécurité n'est pas vraiment un problème et que nous ne devrions pas nous faire trop de souci à son sujet.

Vous avez peut-être confiance, pensant que ces technologies sont en de bonnes mains, vu qu'elles sont utilisées par des services gouvernementaux tenus de rendre des comptes au public. Ou peut-être avez-vous des doutes sur la capacité des autorités de se servir des technologies de sécurité avec compétence, dans le respect de l'éthique et en ayant à cœur les intérêts de tout un chacun dans la société.

Peut-être estimez-vous que ces technologies n'ont pas vraiment d'incidence sur vous : après tout, elles visent d'autres personnes, qui ont mal agi, et sont utilisées dans des lieux où vous n'allez pas. Il se peut cependant qu'à votre avis, chacun devrait se sentir concerné en raison de la quantité de données traitées par ces technologies, et parce qu'elles font de chacun un suspect potentiel. Vous vous sentez peut-être à l'aise quant à l'utilisation qui est faite aujourd'hui de ces technologies, mais êtes inquiet de l'usage qui pourrait en être fait à l'avenir.

Quel que soit votre sentiment sur ces questions, on ne peut pas simplement décider pour tout le monde d'abandonner un peu de vie privée pour un peu plus de sécurité. Le but de SurPRISE est de comprendre la diversité des points de vue sur ces nouvelles technologies de sécurité.

Nous nous réjouissons de vous accueillir au forum de discussion. Si vous souhaitez en savoir plus sur le projet et ses partenaires, nous vous invitons à visiter le site web de SurPRISE <http://surprise-project.eu>.

## Au sujet de ce document

Cette brochure d'information a été produite pour informer les participants des forums de discussion SurPRISE. Cette publication est fournie par l'Institut d'évaluation des choix technologiques (Institut für Technikfolgen Abschätzung) de l'Académie autrichienne des sciences (Strohgasse 45/5, A-1030 Vienne) à tous les partenaires du projet SurPRISE. Pour plus d'informations sur le projet et ses partenaires, veuillez consulter le site web de SurPRISE : <http://surprise-project.eu/>.

- > Auteur : Dr Kirstie Ball, The Open University
- > Conseil consultatif scientifique : Dr Monica Areñas Ramiro, M. Robin Bayley, Pr Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Dr Majtényi László, M. Jean Marc Suchier, Mme Nina Tranø, Pr Ole Wæver
- > Layout : Peter Devine, David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- > Illustrations : David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- > Commanditaire de SurPRISE : 7e programme-cadre de la Commission européenne
- > Cette publication peut être obtenue sous : <http://surprise-project.eu>
- > Comment ce document a été produit : Cette brochure d'information a été écrite par Kirstie Ball en étroite collaboration avec la Danish Board of Technology Foundation, le consortium SurPRISE et son conseil consultatif. Elle a été soumise à quatre révisions internes et à une révision externe et a fait l'objet de tests auprès de groupes au Danemark, en Hongrie et au Royaume-Uni.



## Partenaires du projet

- > Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften (ITA/ÖAW), Coordinateur du projet, Autriche
- > Agencia de Protección de Datos de la Comunidad de Madrid (APDCM)\*, Espagne
- > Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), Espagne
- > Teknologiradet-The Danish Board of Technology (DBT), Danemark
- > European University Institute (EUI), Italie
- > Verein für Rechts und Kriminalsoziologie (IRKS), Autriche
- > Medià Opinion and Market Research Limited Company, Hongrie
- > TA-SWISS/Académies suisses des sciences, Suisse
- > Teknologiradet-The Norwegian Board of Technology (NBT), Norvège
- > Open University (OU), Royaume-Uni
- > Unabhängiges Landeszentrum für Datenschutz (ULD), Allemagne

\* APDCM, die Agencia de Protección de Datos de la Comunidad de Madrid (autorité de la protection des données de la ville de Madrid) était partenaire du projet SurPRISE jusqu'au 31 décembre 2012. En raison de la situation politique régnant en Espagne, la collaboration a pris fin en décembre 2012

# **Surveillance, vie privée et sécurité : une évaluation participative des critères et des facteurs déterminant l'acceptabilité des technologies de sécurité en Europe.**



