



Atelier du CEPD sur la vidéosurveillance au sein des institutions et organes de l'Union

Bruxelles, le 30 septembre 2009

Allocution d'ouverture: les droits fondamentaux en jeu

Giovanni BUTTARELLI

Contrôleur européen adjoint de la protection des données

Chers collègues, Mesdames et Messieurs,

C'est un plaisir pour moi de vous accueillir à cet atelier sur la vidéosurveillance au sein des institutions et des organes européens.

Notre objectif aujourd'hui n'est pas uniquement de collecter vos commentaires constructifs, que nous pourrions utiliser afin d'améliorer le projet de lignes directrices, il s'agit aussi d'intensifier notre coopération dans un domaine – la vidéosurveillance au sein des institutions européennes – qui doit être substantiellement réévalué à la lumière des principes de la protection des données.

Je ferai simplement quelques remarques préliminaires sur la vidéosurveillance et son rapport avec les droits fondamentaux. Nous abordons un domaine qui évolue rapidement et qui, a priori, pourrait sembler très technique et relever exclusivement des technologies de l'information ou de la gestion de la sécurité. Cependant, la vidéosurveillance touche aussi des questions sensibles et stratégiques, dans la mesure où un certain nombre de libertés et de droits sont en jeu.

Je n'entends pas glorifier ici la valeur abstraite des droits fondamentaux par rapport aux besoins en matière de sécurité et de bonne administration. Toutefois, nous ne pouvons pas traiter ces questions en nous basant sur le fait que ce domaine dépend pleinement des choix effectués en matière de sécurité et de technologies de l'information, comme il semble ressortir de la position reflétée dans certains commentaires reçus.

Nous savons tous que la vidéosurveillance est devenue un outil populaire permettant de répondre aux questions ayant trait à la sécurité. Elle se répand également progressivement au sein des institutions et des organes de l'Union européenne qui recourent de plus en plus à cette technologie afin de contribuer à garantir la sûreté de leurs bâtiments et la sécurité du personnel et des visiteurs, ainsi que pour protéger les propriétés et les informations que renferment leurs locaux.

En dépit de sa popularité et des avantages potentiels que revêt la vidéosurveillance, cette technologie suscite néanmoins de graves préoccupations concernant la protection de la vie privée et autres libertés et droits fondamentaux, tels que la protection de la vie privée sur le lieu de travail, la liberté de circulation, le droit à la non-discrimination, la liberté d'expression et la liberté de réunion pacifique, des droits auxquels nous sommes attachés et qu'en Europe nous considérons bien trop souvent comme acquis.

Par exemple, il convient bel et bien de se demander si la liberté de circulation (mentionnée dans de nombreuses chartes constitutionnelles, ainsi qu'à l'article 2 du protocole additionnel n° 4 à la Convention européenne des droits de l'homme) signifie la liberté de circuler non seulement au sens physique, mais aussi d'un point de vue plus fondamental, c'est-à-dire la liberté de circuler sans laisser des traces constantes et/ou fréquentes de nos déplacements dans l'intérêt d'«informateurs optiques» permanents.

En effet, les systèmes de vidéosurveillance sont de plus en plus omniprésents. Ils sont également de plus en plus sophistiqués et puissants. Les systèmes modernes filment et enregistrent des images numériques facilement copiées et diffusées, qui peuvent ensuite être transmises instantanément à une multitude de destinataires, ou même publiées sur l'internet grâce aux puissants réseaux - actuels et futurs - de communications numériques.

Ces enregistrements numériques, contenant un flot continu d'informations détaillées, peuvent aussi très facilement faire l'objet d'archivages, d'indexages et de recherches à des fins de

visionnage et d'analyse illimités. La probabilité que des images soient conservées pour une future extraction de données ne cesse de s'accroître, en raison de la faisabilité technique d'une telle pratique. Des systèmes intelligents et interconnectés sont de plus en plus à même de comparer des images à une base de données d'images, ou encore à suivre des cibles mobiles (objets ou personnes) dans de grands espaces.

Dans certains cas, ces systèmes sont aussi de plus en plus aptes à identifier automatiquement un comportement «suspect» prédéfini. En effet, dans certains domaines, une surveillance automatisée, dynamique et préventive est – ou sera prochainement – capable de remplacer la traditionnelle surveillance statique.

Les caméras elles-mêmes sont également plus puissantes et plus sophistiquées. Les caméras à balayage horizontal, vertical et zoom (pan/tilt/zoom, PTZ) peuvent effectuer des balayages horizontaux et zoomer sur leurs cibles de plus en plus précisément. Les caméras à infrarouges, les dispositifs de détection thermique et autres caméras spéciales peuvent désormais filmer des images dans l'obscurité, y compris à travers les murs ou s'immiscer sous nos vêtements.

À l'échelle internationale, des spécialistes de la surveillance travaillant dans des centres de recherche sur l'imagerie numérique œuvrent en permanence pour concevoir des systèmes de vidéosurveillance toujours plus intelligents dans le but d'améliorer l'efficacité par automatisation.

Ces nouvelles caractéristiques (et d'autres) de la vidéosurveillance, ainsi que l'omniprésence accrue de la technologie elle-même, offrent quantité de possibilités bien réelles, tant en matière de violations de la sécurité que de mauvaise utilisation de celle-ci: les enregistrements peuvent tomber dans de mauvaises mains ou être utilisés par les destinataires légitimes à des fins illégitimes. Si les enregistrements sont conservés pendant une longue période ou envoyés à une multitude de destinataires, il y a un risque de «détournement d'usage»; en d'autres termes, les possibilités d'utiliser les images à des fins qui n'étaient pas initialement prévues et spécifiées sont de plus en plus importantes.

Les risques de la vidéosurveillance vont néanmoins au-delà des cas concrets d'abus ou de mauvaise utilisation. On peut affirmer que le fait d'être observé change notre façon de nous comporter. En effet, lorsque nous sommes observés, la plupart d'entre nous censurons notre discours et notre comportement. Dans le cas d'une surveillance généralisée et constante, le

fait de savoir que nos moindres faits et gestes sont observés par des caméras peut avoir une influence psychologique, étant donné que nous pourrions devoir adapter constamment notre comportement aux attentes de ceux qui nous observent.

Selon la jurisprudence de la Cour européenne des droits de l'homme, cela constitue une intrusion dans notre vie privée, intrusion qui devrait être légitime, justifiée et proportionnée.

En outre, la vidéosurveillance a également des coûts sociaux qui lui sont propres. Elle peut certes décourager les activités criminelles, mais aussi toute autre forme légitime de comportement non conformiste. Cette inquiétude est tout particulièrement justifiée sur le lieu de travail où les travailleurs sont en droit d'attendre ce qu'il est convenu d'appeler une «attente raisonnable en matière de protection de la vie privée».

Nous devons également évaluer les effets possibles sur les protestations politiques, les manifestations et autres formes d'expression protégées à proximité des bâtiments et des institutions, et donc potentiellement dans la zone couverte par leurs systèmes de vidéosurveillance. Dans une société démocratique, l'exercice du droit à la réunion pacifique devrait théoriquement garantir (hormis pour des dérogations justifiées, à analyser au cas par cas) qu'une personne puisse circuler dans la rue anonymement sans laisser un quelconque enregistrement détaillé de son passage.

Les systèmes de surveillance peuvent avoir des effets positifs en matière de sécurité, mais on ne peut uniformément s'accorder à dire que (et dans quelle mesure) ces effets sont globalement positifs. Dans quelques cas, il ne fait aucun doute que le nombre d'infractions pénales dans des lieux publics a été réduit; dans d'autres, cette surveillance s'est avérée inefficace, a incité les contrevenants à se déplacer vers des zones voisines, ou bien a simplement permis d'obtenir des preuves préjudiciables aux personnes filmées.

Il existe des circonstances dans lesquelles il est légitime et nécessaire de sacrifier, dans une certaine mesure, la protection de la vie privée et autres droits fondamentaux dans l'intérêt de la sécurité. Néanmoins, la charge de la preuve doit toujours incomber à ceux qui affirment qu'un tel sacrifice est nécessaire. En effet, nous ne devrions pas troquer des droits fondamentaux contre l'illusion d'une plus grande sécurité.

Quant à la proportionnalité, il convient de ne pas se contenter d'imposer le principe selon lequel il suffit que la surveillance soit liée à des fins «légales» sur la base d'une législation – souvent trop générale – qui pourrait être interprétée de sorte à inclure non seulement les violations du droit pénal, mais aussi les violations des droits administratif/civil/disciplinaire et autres infractions d'ordre plus général. La surveillance devrait être axée sur des aspects qui supposent un risque réel, par exemple les événements publics pour lesquels on peut raisonnablement s'attendre à un risque majeur d'incidents et d'infractions plus graves. Dans le cas contraire, nous errons tels des somnambules dans une société de la surveillance, pas à pas, sans même en réaliser les conséquences: dans une société où nos libertés et nos droits fondamentaux seront considérablement et constamment restreints.

De plus, il convient de noter que l'exigence d'ouverture est parfois respectée en informant simplement le public que des caméras et autres dispositifs de contrôle ont été installés et sont actifs: les personnes concernées sont «contraintes» de fournir des données personnelles (c'est-à-dire souvent des images) et aucune information ne leur est fournie quant à leur utilisation, même si ces données ou images sont incluses dans des dossiers de données ou utilisées à des fins d'identification. Les personnes concernées peuvent dès lors être transformées en «sujets» d'informations, sans aucun respect du droit à l'autodétermination informationnelle.

En conclusion, il est nécessaire d'adopter une approche résolument plus sélective de l'utilisation des systèmes de surveillance: le public dans son ensemble ne doit pas subir de limitations excessives au nom de la nécessité de lutter contre la mauvaise conduite d'une minorité.

La portée du débat, aujourd'hui et dans d'autres forums, devrait dès lors être étendue et aller au-delà de la question des effets bénéfiques sur la sécurité des personnes et de la propriété: une évaluation des effets sur la liberté et la conduite des citoyens serait plus appropriée. En d'autres termes, en plus de chercher à déterminer dans quelle mesure la surveillance entraîne une violation de la protection de la vie privée, il convient d'évaluer les effets résultant de l'utilisation généralisée de la surveillance sur la liberté de circulation et sur le comportement des citoyens.