

# Le paysage en mutation de la liberté et de la sécurité en Europe, un DÉFI

The Centre for European Policy Studies

Bruxelles, le 28 avril 2009

Giovanni BUTTARELLI

---

Je tiens à **remercier le Centre** de m'avoir invité à ce séminaire et je me félicite de voir les questions relatives à la vie privée abordées dans le cadre des présentations. J'ai également apprécié cette invitation à échanger nos points de vue personnels dans un débat très informel à huis clos, ce qui est parfois plus utile.

Permettez-moi de me concentrer d'abord sur **trois affirmations probablement évidentes mais claires,** auxquelles je souscris, à savoir:

a) la protection des données est en effet **une condition préalable** pour faire respecter correctement la loi et l'ordre (public) dans nos sociétés;

b) les services répressifs **doivent respecter** les règles relatives à la protection des données;

c) les autorités de protection des données **devraient être associées** afin d'éviter que ces règles n'entravent la lutte contre la criminalité.

J'aimerais très brièvement dresser un bilan provisoire, vingt ans après la définition des premières règles spécifiques à la protection des données en matière d'activités judiciaires et policières, à savoir l'accord de Schengen de 1985 et la recommandation R(87)15 du Conseil de l'Europe.

Ce faisant, je pourrais évoquer de mauvais résultats, mais également **de bons exemples** d'une relation fructueuse entre la lutte contre la criminalité et des lois rigoureuses sur la protection des données, comme la législation italienne.

Notamment dans mon pays, l'action de l'APD nationale **a parfois eu un effet favorable sur le système policier et judiciaire** chaque fois qu'il a été tiré un avantage mutuel de la possibilité de mener un dialogue approfondi.

Un accès sécurisé à des bases de données très sensibles par le biais de cartes multiservices, la gestion des informations biométriques, les données génétiques, les mesures de sécurité à adopter par les tribunaux, l'accès des citoyens aux dossiers de la police, les inspections sur site des systèmes informatiques: voilà **quelques premiers exemples du scénario européen pour les années à venir** que j'appelle de mes vœux.

En Europe, du point de vue de la protection des données, nous avons probablement tiré **davantage de satisfaction de la première génération de règles** liées à des accords et conventions donnés. Je pense ici au Système d'information Schengen, à Eurodac, à Europol ou à la convention de Dublin sur la politique d'asile.

À cette époque, les autorités de protection des données avaient **moins d'occasions** d'être officiellement consultées et associées aux négociations pertinentes. Néanmoins, des garanties suffisantes ont été instaurées, parfois de façon un peu traditionnelle ou dans le cadre

d'une approche officielle, mais en tout cas pour un résultat **assez équilibré**.

En revanche, en matière d'équilibre entre le respect de la vie privée et la sécurité, **certaines expériences plus récentes** dans le premier et le troisième pilier, par exemple concernant l'affaire PNR (dossier passager) ou SWIFT, **n'apparaissent pas pleinement satisfaisantes** en comparaison aux expériences passées, malgré les multiples contributions émanant des divers forums traitant de la protection des données.

Chacun de nous peut avoir une **idée différente et subjective** de ce qui constitue un équilibre approprié entre les droits et libertés fondamentaux et la sécurité publique. Mais en toute hypothèse, il est **temps d'entamer un nouveau débat organique et proactif** sur l'efficacité de la gestion des informations dans le cadre des activités policières et judiciaires dans toute l'Europe.

Nous pourrions vérifier tous ensemble s'il y a **trop ou trop peu de bases de données répressives**, qu'elles soient parfois assez statiques ou dynamiques.

Concernant ce qu'il se passe en Europe, permettez-moi de vous dire que, de mon point de vue tout à fait personnel, nous disposons probablement, de manière générale, de peu de bases de données vraiment intelligentes en vigueur.

Permettez-moi également de vous dire – en ma qualité de juge – que nos forces policières et nos autorités judiciaires ne disposent pas toujours de tous les instruments appropriés pour prévenir et combattre la criminalité. En effet, la lutte contre la criminalité requiert efficacité et rapidité.

Mais en partant de ce constat, nous ne pouvons commettre l'erreur d'oublier le citoyen lambda ou de ne pas promouvoir ses droits, ses libertés et sa dignité.

À mon sens, une approche intelligente de la protection des données au sens contemporain du concept devrait être particulièrement utile pour trouver la légitimité démocratique d'une politique plus efficace en matière de données policières.

La protection des données en tant que telle n'est qu'un des facteurs pouvant influencer la collecte et le traitement de bonnes informations dans un fichier policier ou judiciaire.

Il convient en effet d'évaluer de nombreux autres facteurs pour vérifier l'actuel niveau de qualité des informations échangées à des fins d'application de la loi, y compris certains flux de données lents ou certaines bureaucraties ou, malheureusement – permettez-moi de parler de nouveau en ma qualité de juge – certaines jalousies ou concurrences dans la promotion et l'application de l'échange d'informations au niveau international.

Certaines informations sont disponibles mais ne sont pas vraiment utilisées ou échangées et leur utilisation est parfois exclue du fait de règles spécifiques en matière de coopération judiciaire plutôt que pour des motifs relevant de la protection des données.

Je souhaite mieux comprendre s'il y a un chevauchement à propos de certaines bases de données

répressives, quel type d'autres initiatives fructueuses l'on peut promouvoir afin d'obtenir des données policières plus actualisées avec une nouvelle évaluation préventive de l'impact sur les libertés et droits fondamentaux.

Le respect de la vie privée dès la conception. Trop de données signifient parfois peu de données.

Par exemple, on pourrait ressentir à tort le besoin d'obtenir et de collecter de nouvelles informations déjà disponibles ailleurs.

De nouveau, nous ne pouvons exclure qu'il faille apporter des modifications à certaines modalités d'interconnexion ou à certaines dispositions qui excluent actuellement d'autres utilisations des données au niveau international ou national.

Mais la protection des données est et devrait rester un élément clé pour renforcer la disponibilité de données pertinentes et non excessives à des fins de sécurité.

Je compte sur les autres parties prenantes pour consentir davantage d'efforts afin de comprendre la

**nécessité d'une politique intelligente et non formaliste en matière de protection des données.**

Nous pourrions tous soutenir **une nouvelle génération de règles en matière de protection des données, plus proches de la substance du problème** plutôt que des formalités, et offrant des **garanties concrètes** au lieu d'un **rappel abstrait** de principes généraux qui ne sont pas respectés.

Nous devons encourager l'application concrète des **principes de nécessité** (qui doit guider l'utilisation de données à caractère personnel et d'identification en minimisant leur traitement si les objectifs poursuivis peuvent être atteints en utilisant des informations anonymes ou n'identifiant pas la personne) **et de transparence** (qui dicte que toute catégorie de traitement de données à caractère personnel doit être transparente en application de la loi).

Les nouvelles technologies et les nouvelles applications techniques pourraient être utiles à cet égard.

Pourquoi ne pas, par exemple, réfléchir à la mise en œuvre utile du **principe de «guichet unique»**, selon lequel les données sont stockées en un seul endroit auquel les autres organes et l'administration pourraient accéder rapidement par le biais de réseaux, sans reproduire toutes les données à un autre endroit dans le cadre d'une approche de masse et en traçant en toute hypothèse les accès en ligne en deux endroits (la partie qui communique les informations et celle qui les reçoit)?

Pourquoi ne pas promouvoir l'augmentation du **nombre de responsables en matière de respect de la vie privée** dans le domaine des bases de données policières et judiciaires?

Pourquoi ne pas encourager **la mise en œuvre effective de technologies de protection de la vie privée** pour qu'un nombre bien plus important d'outils automatiques puissent prévenir certaines violations des règles en matière de protection des données?

Il faut s'attendre à devoir consentir davantage d'efforts pour **distinguer les données liées aux aspects**

**administratifs de la vie quotidienne** (un numéro de permis de conduire, par exemple) **et les données concernant des comportements criminels**, en tenant également compte des **conséquences potentielles pour les citoyens normaux** comme le fait d'être inscrit sur une liste d'interdiction de vol.

Les autorités de protection des données doivent expliquer dans **un nouveau langage proactif** comment mieux appliquer les principes de légalité, de finalité et de proportionnalité aux activités de sécurité.

Il faut promouvoir l'adoption de **nouvelles règles faciles d'utilisation, techniquement avancées, concrètes et non bureaucratiques.**

En suivant de près l'évolution technologique dans les **nouveaux domaines** comme la génétique, la localisation et la surveillance intelligente, nous devons tous prendre les décisions pertinentes **qui ne peuvent aucunement être déléguées aux outils technologiques.**

Tout ce qui est techniquement faisable n'est pas forcément socialement acceptable, éthiquement admissible ou légalement permis.

Davantage de sécurité pour les citoyens signifie également davantage de protection pour les données.

Je vous remercie de votre attention.

Giovanni BUTTARELLI