« Communiquer sur la protection des données et la rendre effective »

Origine de cette initiative

Cette initiative repose sur le discours prononcé par Alex Türk, Président de l'autorité française de protection des données, lors d'une conférence organisée à Varsovie en mai 2006 par l'Inspecteur Général à la Protection des Données polonaise, sur le thème « Sécurité publique et protection des données ». Dans ce discours, Alex Türk exprimait sa vive préoccupation face aux défis auxquels sont actuellement confrontées les autorités de protection des données dans le monde. Il insistait sur la nécessité absolue que les autorités infléchissent leur action pour répondre à ces défis, si l'on ne veut pas voir la philosophie qui sous-tend les règles de protection des données privée de sa substance.

A la suite de cette conférence, le Contrôleur européen a invité la CNIL à développer une initiative commune exposant l'urgence d'une nécessaire action et visant à provoquer une prise de conscience collective, qui serait présentée à la conférence internationale de Londres. L'Information Commissioner britannique a immédiatement soutenu cette initiative. Ce texte a été rédigé en étroite collaboration entre ces trois autorités.

En adhérant à cette initiative, les autorités participantes s'engagent à coordonner leurs actions pour contribuer à cette prise de conscience, notamment en :

- accentuant leurs activités de communication, sur la base d'idées communes, dont certaines sont évoquées dans le texte ci-joint ;
- adaptant leurs pratiques et méthodes de travail, grâce à l'évaluation de leur efficacité et au renforcement de leurs capacités d'expertise, de prospective et d'intervention dans le champ technologique ;
- contribuant à faire reconnaître l'action de leurs autorités de manière institutionnelle, sur le plan international et à promouvoir l'implication de tous acteurs appropriés sur les plans national et international.

A l'heure actuelle, les autorités de protection des données suivantes ont en principe apporté leur soutien à cette initiative :

- Commission nationale de l'informatique et des libertés (France)
- Contrôleur européen à la protection des données (Union Européenne) ;
- UK Information Commissioner (Royaume-Uni) ;
- Commissaire fédéral à la protection de la vie privée (Canada);
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Allemagne);
- Agencia Española de Protección de Datos (Espagne);
- Garante per la Protezione dei Dati Personali (Italie) ;
- College Bescherming Persoonsgegevens (Pays-Bas);
- Privacy Commissioner (Nouvelle Zélande);
- Préposé fédéral à la protection des données et à la transparence / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Suisse).

Cette initiative conjointe sera présentée lors de la session fermée de la conférence internationale des commissaires à la protection des données, qui se tiendra à Londres les 2 et 3 novembre prochains. Elle ne sera pas présentée pas la forme d'une résolution. Elle sera présentée comme une initiative conjointe de la CNIL, du Contrôleur européen et du UK Information Commissioner, que soutiennent les différentes autorités mentionnées plus haut, qui se seront engagées à adapter leurs actions en conséquence. Les autres autorités présentes à la Conférence seront invitées à exprimer leur soutien,

voire à se rallier à cette initiative si elles le souhaitent. Il n'est pas prévu que ce document soit formellement adopté par la conférence.

Après avoir rappelé pourquoi la protection des données est indispensable à une société (I), ce texte analyse dans le détail les risques qui pèsent aujourd'hui sur les libertés individuelles et la protection des données dans le monde, et qui représentent autant de défis pour les autorités de contrôle (II). Il tire de ce constat différentes propositions d'actions et d'initiatives coordonnées (III), ainsi que le développement d'une nouvelle stratégie commune de communication (IV).

I – LA PROTECTION DES DONNEES EST INDISPENSABLE A UNE SOCIETE

1. La protection des données personnelles de nos citoyens est un impératif vital pour une société, au même titre que la liberté de la presse ou la liberté d'aller et venir. Nos sociétés sont de plus en plus dépendantes des nouvelles technologies, et les données à caractère personnel sont collectées ou générées dans des proportions sans cesse plus importantes. Il en devient d'autant plus essentiel que les libertés individuelles et les autres intérêts légitimes des citoyens soit respectés de manière adéquate dans les traitements de l'information.

2. La protection des données n'est pas, ne doit pas être conçue comme un thème abstrait, théorique, voire même « théologique ». Les règles de protection des *données* protégent des *personnes*. Il s'agit de protéger un droit à ne pas être fiché, surveillé, contrôlé de manière abusive et incontrôlée ; il s'agit de protéger la dignité humaine, de permettre aux personnes d'exercer leurs droits et que leurs intérêts légitimes soient préservés.

3. La protection des données ne peut être une réalité que si les règles de protection des données sont respectées en pratique. Les autorités de protection des données jouent un rôle fondamental à cet égard. Cependant elles ne joueront ce rôle qu'en communiquant de manière efficace sur la protection des données, en impliquant les acteurs concernés, et si nécessaire en faisant usage de leurs pouvoirs de contrôle et de mise en œuvre.

II – DEUX VAGUES ; UN TRIPLE DEFI

4. Les libertés individuelles et nos autorités sont exposées à des risques sans précédents ; elles sont menacées de manière irréversible par deux vagues, et doivent faire face à un triple défi.

A - Le premier défi est d'ordre technologique, du fait d'une combinaison de facteurs

5. **Le facteur « accélération »** : Internet, RFID, nanotechnologies, etc. Les autorités ne sont pas hostiles au progrès technologique. Mais les délais entre la découverte d'un phénomène et sa mise en œuvre technologique se raccourcissent et le temps de passage d'une innovation à une autre innovation, du développement d'un prototype à son déploiement industriel, se réduit sans cesse. Il devient de plus en plus difficile de faire coïncider l'adaptation ou l'interprétation des règles de droit à l'évolution technologique : le temps technologique accélère sans cesse, tandis que le temps juridique reste particulièrement lent, régi par le rythme des procédures démocratiques.

6. **Le facteur « globalisation »**: les délocalisations de traitements de données sont en plein essor. Il est indéniablement devenu extrêmement difficile, sur le plan international, de contrôler les échanges de données. Cette tendance à la globalisation est souvent en conflit avec

une grande caractéristique de la règle de droit, à savoir un champ d'application étroit, limité à un territoire et à un champ de compétence ordonné et balisé.

7. **Le facteur « ambivalence »**: l'innovation technologique est porteuse de progrès comme de dangers. Autant les individus sont tentés par le confort qu'elle procure, autant ils sont peu conscients des risques qu'elles comportent, du moins jusqu'à ce qu'ils en soient victimes ou qu'il soit trop tard : ils ne se préoccupent pas de leur traçabilité, de la surveillance potentielle de leurs déplacements, de leurs comportements, de leurs relations. Cette ambivalence de la technique est difficile à concilier avec la règle juridique qui doit, par définition, être univoque, et se trouve, bien souvent, en inadéquation avec cette ambivalence du progrès technique.

8. **Le facteur « imprévisibilité » :** les usages de la technologie se développent souvent de manière imprévisible, y compris parfois pour leurs concepteurs. Les usages imprévus d'une technologie peuvent, de ce fait, être difficiles à encadrer, surtout quand ils divergent des usages pour lesquels celle-ci avait été initialement conçue, et pour lesquels la loi semblait en mesure de s'appliquer.

9. **Le facteur « invisibilité » (Invisibilité virtuelle / Invisibilité physique ou réelle)** : Le traitement de l'information est de plus en plus « invisible », impalpable, de moins en moins maîtrisable. La technologie tend à devenir invisible non seulement du fait de plus en plus de traitements de données virtuels sont réalisés à l'insu des personnes (traçabilité des déplacements physiques dans les transports en commun, des consultations sur Internet, des communications téléphoniques, etc.) : c'est l'invisibilité virtuelle, liée aux processus. Elle tend aussi à devenir invisible du fait de son extrême miniaturisation : c'est l'invisibilité physique ou réelle. Dans quelques années, avec les nanotechnologies, il sera devenu impossible de voir à l'œil nu que la technologie est présente dans un objet : comment encadrer et contrôler des traitements effectués par le recours à une technologie invisible ?

10. **Le facteur « irréversibilité »** : Le progrès technologique est irréversible : nous ne vivrons plus jamais dans un monde sans ordinateurs, sans Internet, sans téléphones portables, sans identification biométrique, sans géolocalisation, sans vidéosurveillance. Ces technologies tendent au contraire à s'imbriquer les unes dans les autres, et les synergies qu'elles créent sont des plus dangereuses pour nos sociétés.

B - Le second défi est d'ordre normatif, lié aux nouvelles législations de lutte antiterroriste

11. Le développement des législations anti-terroristes lance un défi aux autorités de protection des données qui, dans ce contexte, doivent éviter les pièges, dénoncer les illusions et combattre les mythes.

12. **Le piège du manichéisme** : ni législateur, ni juridiction, ni association militante, les autorités indépendantes de protection des données ont un rôle très particulier à jouer. Il leur sera rarement possible de résoudre un problème de manière tranchée, « blanc ou noir ». Ainsi, l'ensemble des autorités de protection des données reconnaît la légitimité des politiques de lutte anti-terroriste mises en œuvre depuis quelques années. Mais elles doivent également, conformément aux missions qui leur ont été confiées par les textes fondateurs, et au nom de la société, rechercher en permanence un équilibre entre les impératifs de sécurité publique, d'une part, et les exigences de la protection de la vie privée et des données personnelles, d'autre part. Elles doivent assumer ce rôle en toute indépendance, et rejeter les accusations inacceptables d'irresponsabilité qui sont parfois portées à leur égard en la matière.

13. **Le risque de l'engrenage :** ce risque est le suivant. Le législateur crée une base de données à un moment donné, dans des circonstances données. L'autorité de contrôle est associée à son

développement. Ultérieurement, le législateur envisage d'étendre le périmètre de cette base – par exemple en étendant d'abord catégories de personnes concernées, puis les motifs d'inscription dans le fichier, puis enfin les catégories de personnes pouvant le consulter… Les promoteurs de ces modifications ultérieures font valoir à l'autorité qu'elle ne peut s'opposer à une simple extension, puisqu'elle a accepté le principe de la création du fichier de base, et ainsi de suite si nécessaire… Ainsi, entre la première et la dernière étape du développement d'un fichier, il se sera opéré un glissement qui remettra fondamentalement en question l'équilibre acceptable de son périmètre d'origine.

14. **L'illusion de « l'exemplarité » :** les exécutifs nationaux invoquent souvent le fait que d'autres pays ont déjà mis en place un dispositif pour reprocher aux autorités de contrôle de tel ou tel pays leur réticence à l'accepter sans discuter. Cela pose de réels problèmes d'harmonisation et rend nécessaire de recourir à des raisonnements fondés sur la définition de dénominateurs communs.

15. **Le mirage du fichier « remède miracle »** : les autorités doivent rappeler sans cesse au public et aux exécutifs que la création d'un fichier informatique comportant toujours davantage de données ne règle pas tout. Il faut désacraliser le caractère supposé infaillible du fichier informatique. Quand de plus en plus de données personnelles sont enregistrées, les risques d'identification erronée, de données périmées et autres erreurs augmentent. Ceci peut causer de véritables préjudices aux personnes, que ce soit pour leur santé, la possibilité d'effectuer des choix de vie, leur prospérité, voire même leur liberté.

16. **Le mythe du fichier infaillible (la problématique « majorité / minorité »)** : il est trop souvent supposé - à tort - que les personnes enregistrées dans une base de données le sont pour une raison valable. Il en résulte que les personnes qui figurent dans ces fichiers de manière indue (« la minorité ») se retrouvent dans une situation parfois dramatique, car tout portera à croire qu'il est impossible d'être dans ce fichier, aussi performant technologiquement, sans que cela soit justifié. Ainsi il est indispensable, sur le plan éthique, de continuer à affirmer que l'informatique peut être faillible et de proscrire la prise de décision automatisée, tout particulièrement dans des domaines comme la sécurité ou la justice.

C - Le troisième défi est celui de la réputation de la protection des données

17. Au moins dans un certain nombre de pays, la protection des données et les autorités de protection ne jouissent pas de la réputation positive qu'elles méritent. Les règles de protection des données peuvent être perçues comme complexes et difficiles à appliquer de manière cohérente, prévisible et réaliste. D'autres critiquent les règles de protection des données comme trop abstraites, et pas assez recentrées sur les dommages réels ou supposés – causés aux personnes ou à la société dans son ensemble – si ces règles ne sont pas observées. D'autres encore critiquent la manière dont ces règles sont interprétées ou mises en œuvre, ce qui les dissuade de se mettre en conformité ou d'investir dans des efforts de mise en conformité. De telles perceptions négatives peuvent être celles d'hommes politiques, d'administrations, d'entreprises, des médias mais aussi de particuliers. Il est nécessaire de combattre ces perceptions, en démontrant l'importance pratique de la protection des données, en matérialisant la réalité des droits et libertés fondamentaux, et en reconsidérant certaines pratiques, si cela s'avère nécessaire.

III – LIGNES D'ACTION ET INITIATIVES POUR LES AUTORITES DE PROTECTION DES DONNEES

18. Devant la gravité des risques énoncés ci-dessus, les autorités de protection des données doivent, de manière urgente, se donner les moyens de provoquer une prise de conscience collective quant aux risques de destruction irréversible qui menacent les libertés individuelles dans leurs pays. Elles doivent aussi évaluer leurs méthodes de travail et améliorer leur efficacité.

A - Les autorités doivent ensemble proposer des réformes et des stratégies coordonnées pour agir mieux, plus efficacement et de manière plus ciblée

19. **Développer la capacité d'expertise, de prospective et d'intervention dans le domaine technologique** : la protection des données « souffre » aujourd'hui de son image excessivement juridique ; or la crédibilité de nos institutions est et sera de plus en plus liée à notre capacité à comprendre et à anticiper les développements technologiques.

20. Pour analyser ces nouveautés, nos autorités doivent élaborer des stratégies de division du travail en fonction des enjeux, des expériences, des responsabilités, des moyens qui sont les leurs.

21. Elles doivent réfléchir aux relations qu'elles souhaitent entretenir avec chercheurs et industriels dans le domaine des technologies de l'information et de communication. Elles doivent présenter aux entreprises et aux administrations la valeur de la protection des données et les bénéfices qu'elles peuvent en attendre.

22. **Évaluer notre efficacité et adapter nos pratiques** : il est absolument nécessaire de procéder à une évaluation sans fard de l'efficacité respective de nos autorités. Notre action a-telle un impact réel, faisons-nos une différence en pratique ? Les mots se traduisent-ils par une réalité? De telles évaluations nous permettront de tirer des leçons pour améliorer nos résultats.

23. L'évaluation de l'efficacité de nos autorités mènera sans doute certaines autorités à revendiquer que le législateur les dote de pouvoirs dont elles ne disposeraient pas. Elle pourra aussi remettre en cause des pratiques de fonctionnement au sein de nos autorités. Celles-ci doivent concentrer leur action prioritairement sur les principaux risques existants aujourd'hui, et veiller à ne pas être d'une rigidité excessive sur des sujets qui ne le méritent pas. Elles doivent être prêtes à faire preuve de davantage de pragmatisme et de souplesse.

B - Les autorités doivent réfléchir ensemble pour faire reconnaître leur action de manière institutionnelle sur le plan international et impliquer d'autres acteurs

24. **Une nécessaire structuration de la Conférence Internationale :** la Conférence Internationale des Commissaires à la Protection des Données doit devenir le fer de lance de l'action de nos autorités sur le plan international. Il faut en assurer la viabilité, en améliorer le fonctionnement, la rendre plus visible et plus efficace, la faire vivre au long de l'année, élaborer un plan d'action, un programme de communication. Ceci impliquera sans doute de réfléchir à la création d'un secrétariat permanent. La conférence doit devenir, sur le plan international, un acteur incontournable dans le traitement d'initiatives internationales ayant une incidence sur le droit de la protection des données ; elle doit permettre la discussion et la remontée d'idées concrètes, afin de mieux suivre les développement internationaux, d'harmoniser les pratiques et d'adopter des positions communes.

25. **Elaboration d'une Convention Internationale** : par la déclaration de Montreux, les Commissaires à la protection des données appelaient au développement d'une Convention universelle de protection des données. Cette initiative doit être soutenue auprès des institutions compétentes par nos autorités, dans le respect de leur positionnement institutionnel et, si nécessaire, après coordination entre autorités compétentes au niveau national. Nos autorités doivent promouvoir cette initiative dans leurs sphères d'influence respectives, en particulier au sein des organisations régionales ou des zones linguistiques auxquelles elles appartiennent. Il pourra s'avérer nécessaire de développer des solutions globales pour le respect de la protection de la vie privée et des données personnelles dans des domaines spécifiques (ex : gouvernance de l'Internet ; transactions financières ; transport aérien) ; ces questions devront être traitées par les autorités par tous moyens appropriés.

26. **Participation d'autres acteurs (société civile ; ONG)** : d'autres acteurs de la protection des données et de la vie privée sont aujourd'hui actifs, sur le plan national comme sur le plan international, à différents niveaux et dans différents secteurs. De telles organisations pourraient être des partenaires stratégiques et contribuer de manière substantielle à l'amélioration de l'efficacité de nos autorités. La coopération avec d'autres acteurs doit ainsi être encouragée, parfois même activement développée.

IV – POUR UNE NOUVELLE STRATEGIE DE COMMUNICATION

27. La communication est un facteur clé pour rendre la protection des données plus effective. Un message qui n'est pas reçu ou reste incompris est un message inutile. Un avis ou une décision qui n'est pas accessible aura un impact limité et ne vaudra pas les efforts nécessaires à le développer.

A - Nous devons, de manière urgente, concevoir et mettre en œuvre une nouvelle stratégie de communication, sur le plan national et sur le plan international

28. **Un objectif : communiquer.** Une meilleure communication vers le public doit être un objectif prioritaire de nos autorités. Il n'est pas concevable que dans certains de nos pays où l'on inscrit le droit à la protection des données parmi les droits fondamentaux imprescriptibles tels que la liberté d'aller et venir ou la liberté de la presse, l'immense majorité de nos concitoyens n'ait aucune conscience d'en être titulaires, ni de leur importance. Ceci est d'autant moins acceptable que la protection des données peut même avoir une réputation négative.

29. Nous devons nous engager dans un puissant effort de pédagogie, et à long terme, visant à informer les personnes de l'existence et du contenu de ces droits. L'effet de ces actions doit être mesurée. Deux catégories doivent être visées en priorité :
    - Les élus nationaux et locaux qui ont, par nature, une responsabilité particulière en la matière et dont l'information doit être améliorée;
    - Les jeunes générations qui font preuve d'une grande indifférence vis-à-vis de ces questions tant ils sont habitués à manipuler ces nouvelles technologies. Il faut donc agir dans le secteur éducatif le plus tôt possible.

30. **Un levier d'action : communiquer**. Il est important et urgent de doter les Autorités de meilleurs moyens d'action et de leur assurer une reconnaissance sur le plan international. La confiance et le soutien du public sont absolument essentiel. La protection des données doit être rendue plus concrète. Seules les organisations communiquant de manière compréhensible, accessible et parlante au grand public, généralement via les médias, disposeront de la puissance nécessaire pour influencer les opinions publiques, et donc pour être entendues et

prises au sérieux par les Etats et la communauté internationale. C'est à cette condition qu'ils pourront obtenir ces moyens d'action indispensables.

31. Ceci passe par une professionnalisation de la fonction de la communication au sein de nos autorités, et par le fait que les messages de communication émis par nos autorités soient cohérents entre eux.

B - Une piste intéressante consisterait à reprendre dans nos activités de communication la notion de capital à préserver, par analogie avec le thème du capital naturel de notre planète mis en danger par la pollution issue de l'activité humaine

32. De même qu'on ne peut pas agir impunément en matière de protection de l'environnement, nous devons être extrêmement vigilants dans notre domaine, à l'égard de toute avancée technologique non maîtrisée comme de toute mise en œuvre de normes nouvelles consenties plus ou moins consciemment, parce que ce capital de garantie de nos libertés et de notre identité peut alors être amputé ou menacé dans son existence même. Et il ne se renouvellera pas, précisément en raison du phénomène d'irréversibilité des effets du progrès technologique.

33. La protection des données est peut-être aussi précieuse que l'air que nous respirons. Tous deux sont invisibles, mais les conséquences sont tout aussi désastreuses quand ils viennent à manquer.

V – PROGRAMME D'ACTIVITES DE SUIVI

34. La discussion de cette initiative lors de la session fermée de la conférence internationale des commissaires à la protection des données et à la vie privée de Londres doit être la première occasion d'élaborer un consensus sur la nécessité d'une action, sur le développement de moyens pour une meilleure communication, et pour faire en sorte que la protection des données soit une réalité.

35. Les autorités soutenant cette initiative s'engagent à participer, et si nécessaire à être responsable d'un certain nombre d'activités communes, telles que :
    - Un atelier sur les questions stratégiques : conditions pour rendre la protection des données plus effective ; développement éventuel de principes de « bonne supervision » en matière de protection des données ; information sur les bonnes pratiques ; réflexion sur le développement d'une convention internationale (commissaires et services) ;
    - Un atelier sur la communication : expertise disponible en matière de communication sur la protection des données (ex : campagnes média ; enquêtes d'opinion) ; développement d'un message commun et d'outils pour le répandre (responsables communication) ;
    - Un atelier sur la mise en œuvre des règles de protection des données : expertise disponible pour s'assurer du respect des règles et le contrôler ; moyens efficaces d'inspection - y compris audits - et d'intervention (commissaires et services des contrôles) ;
    - Un atelier sur l'organisation interne des autorités : expériences récentes en matière de changement organisationnel ; projets d'amélioration de l'efficacité de l'autorité (commissaires et services en charge de l'organisation de l'autorité) ;
    - Toute autre activité pertinente pour cette initiative.