

Journée internationale de la protection des données

Université de Lausanne, le 28 janvier 2022

Allocution de Adrian Lobsiger, préposé fédéral à la protection des données et à la transparence

STRATEGIE ET PROJETS DE TRANSFORMATION NUMERIQUE

Mesdames, Messieurs,

Chers collègues,

Je suis très heureux de célébrer cette année la Journée internationale de la protection des données avec mes collègues des cantons francophones et des cantons bilingues, ici à Lausanne.

1. Nos défis

Comme autorités de protection des données nous sommes confrontés à des défis comparables, et ce dans toute la Suisse :

- Une numérisation qui progresse de manière dynamique, avec des pannes et des fuites de données qui nous tiennent occupés ;
- Une pandémie qui dure depuis deux ans et qui entrave la vie privée et autodéterminée de la population – pensons au télétravail obligatoire et à la surveillance électronique à domicile qui peut en découler, ou encore au certificat Covid qui a transformé le smartphone en bracelet électronique ;
- Il s'agit d'une pandémie qui nous met doublement au défi, en ce sens que notre propre personnel est également touché par la maladie et que son travail, déjà exigeant et interdisciplinaire, est rendu plus ardu ;
- Dans ce contexte, j'aimerais exprimer ma gratitude à toutes les collaboratrices et collaborateurs de nos autorités fédérales et cantonales pour leur engagement quotidien dans des conditions difficiles ;

2. Notre obstination

Ce qui nous unit, c'est notre « volonté tenace », en tant qu'autorité de surveillance indépendante et apolitique, d'agir dans la réalité numérique en faveur de la population.

- Je dis « volonté tenace » parce que nous accomplissons cette tâche avec des ressources humaines modestes, et pour certains d'entre nous quasi inexistantes. En général, nous voyons des budgets qui semblent dérisoires par rapport aux investissements que l'État affecte à la numérisation de ses administrations.

- « Notre volonté tenace », je le répète, car ceux qui s'attendent secrètement à ce que nous disparaissions dans le tourbillon de la croissance numérique doivent bien constater que nous continuons à nous exprimer.

- « Notre volonté tenace », je le redis, parce que nous restons sereins, objectifs et crédibles dans nos déclarations et nous ne cédon's ni aux provocations des politiciens, ni à celles des médias, ni aux pressions des réseaux sociaux. Et nous ne nous laissons pas non plus aller à des jugements prématurés ni à des minimisations.

3. Transformation numérique

Les nombreux projets de transformation numérique des administrations actuellement en cours aux niveaux fédéral, cantonal et communal sont de grande actualité.

Cette transformation n'est pas remise en question par la protection des données. Mais elle crée un rapport de tension avec la règle de la séparation et de la limitation des pouvoirs et le fédéralisme sur lesquels repose notre État de droit. Des principes que certains promoteurs de projets numériques traitent avec une ignorance quasiment infantile. Je parle d'une idée fixe de transférer toutes les données - sans distinction claire entre données personnelles et non personnelles - dans des nuages numériques auxquels tous les services publics auraient accès.

Ils n'arrêtent pas de parler de « silos de données » qui feraient obstacle à la numérisation du pays et auraient dû être supprimés depuis longtemps. La phobie des « silos » risque de nous pousser dans un Disneyland doté d'un nuage numérique rose qui perfectionnerait l'État numérique, qui se transformerait – c'est ma crainte - en Etat policier. Etat policier que nous pensions avoir surmonté depuis l'abolition de la monarchie absolue.

4. État policier numérique ?

Avons-nous déjà oublié que c'est la scission de l'État de l'Ancien Régime en entités spécialisées qui a créé les conditions propices à l'émergence du service public et à la transformation des sujets en citoyens ? Aujourd'hui, nous faisons tous partie d'une société civile qui exige de chaque service des prestations professionnelles et discrètes en échange des taxes que nous payons. Si, dans le cadre de projets de transformation numérique, les autorités de police, de renseignement, les administrations douanières, fiscales et anti-blanchiment commencent à recouper leurs données et à accéder à leur guise aux informations des autres autorités, la confiance dans ce « service public numérique » sera rapidement détruite.

5. Analyse d'impact de risque

C'est ce risque de mise en relation indifférenciée des données menaçant l'État de droit qui est en jeu lorsque nous évoquons les instruments modernes de la protection des données. Selon les nouvelles lois que la Confédération et les cantons vont bientôt mettre en vigueur, les projets de transformation de l'administration doivent être précédés d'une analyse d'impact de risques. Ces analyses ne doivent pas se limiter à des détails de sécurité technique visant à empêcher les accès non autorisés. Dans leurs projets de transformation numérique, les administrations doivent également démontrer de manière claire et contraignante en quoi les traitements de données actuels se distinguent des traitements prévus. Ce faisant, elles doivent également faire la différence entre les données personnelles et les autres données. Ce n'est qu'ainsi que l'intensification inaperçue du traitement des données des citoyens pourra être mise en lumière. Comme je le sais par mon expérience pratique, c'est un éclairage que de nombreux promoteurs du changement numérique fuient. Ils préfèrent se réserver toutes les options de ce qui est techniquement faisable en invoquant la soi-disant « agilité » de leurs projets.

6. Régimes autoritaires

Or, la protection des données ne vise pas à la conservation des monuments historiques, mais à la préservation des droits fondamentaux dont les humains sont privés dans les États autoritaires. Dans ces pays, les gens doivent s'attendre à ce que l'administration leur interdise du jour au lendemain l'accès à l'éducation, aux soins, aux assurances ou aux services publics sur la base d'informations partagées avec la police, les renseignements ou d'autres autorités. Grâce à la mise en réseau

numérique et à la technologie de surveillance bon marché, nombre de ces États ont entre-temps intensifié le contrôle de leur population dans une mesure telle qu'elle effraiera encore longtemps, espérons-le, l'Occident.

Si les autorités policières, douanières et de renseignements suisses veulent se démarquer de manière crédible de ces pratiques autoritaires, je ne peux que leur conseiller d'autoriser un minimum de transparence, par exemple en ce qui concerne l'acquisition de technologies de surveillance. Si le changement numérique est conçu dans des sphères marquées par le secret de fonction et le secret commercial, il perdra le capital confiance de la population.

7. Stratégies numériques

Regardons par exemple un projet de législation sur l'intelligence artificielle, récemment publié par l'Union Européenne, qui interdit aux États membres la surveillance permanente de la population sous forme de notation sociale ainsi que l'utilisation généralisée de systèmes de reconnaissance faciale dans l'espace public en temps réel. Du point de vue de la protection des données, on ne peut qu'être d'accord. Sauf que nous devrions également prendre en compte les exceptions devenues courantes dans ce genre de stratégies numériques. Des exceptions au profit de la lutte contre le terrorisme et de la poursuite pénale ainsi que de la protection des victimes et des enfants. Des exceptions qui montrent comment la technologie de surveillance disponible dans le monde entier et la pression pour la mise en réseau numérique laissent des traces en Occident. Certes, la « protection des données » repose toujours sur un piédestal.

8. Piédestal stratégique

C'est encore le cas parce que la « sécurité technique » des données est indispensable à cause de la cybercriminalité galopante. Mais que se passera-t-il si les particuliers « sécurisent » réellement leurs données et les isolent de l'État au moyen du cryptage ?

9. My data ?

Des ennuis menacent, également en Occident, ceux qui veulent rendre inaccessibles leurs données.

Il y a quelques mois, Apple a annoncé, le plus sérieusement du monde, en invoquant la protection des enfants, son projet de fouiller les images de tous les smartphones

en recourant à l'intelligence artificielle et de dénoncer les propriétaires de ces appareils à la police. Les critiques publiques que le groupe s'est ainsi attirées à juste titre devraient servir d'avertissement à l'ensemble de l'économie de technologie. Elle doit veiller à ne pas se transformer en complice docile des autorités de sécurité sous l'influence de stratégies numériques ambiguës.

10. Notre obstination

Nous aborderons certainement d'autres risques liés au changement numérique au cours de la discussion. Je ne considère pas qu'il est de mon devoir de diaboliser le changement numérique et je n'ai pas non plus la vocation de faire peur aux gens. Comme je viens de le dire, il me semble plutôt que nous devons continuer à faire preuve d'« obstination » pour que les nombreuses opportunités incontestées de la numérisation soient enfin évaluées en fonction des risques pour notre vie privée et notre autodétermination numérique.

* * *