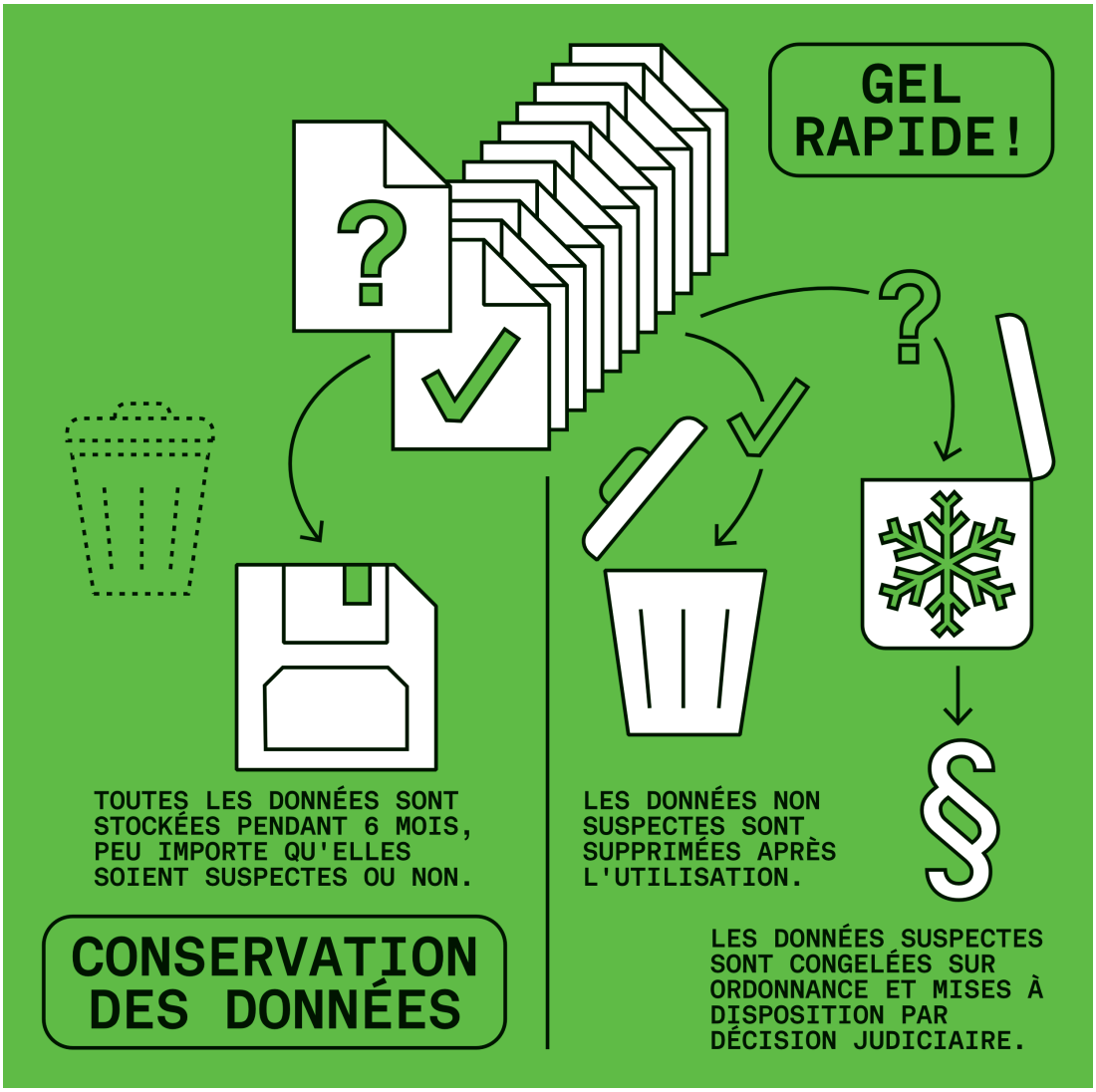
SOCIETE NUMERIQUE

«GEL RAPIDE» AU LIEU DE LA CONSERVATION DE DONNÉES

UNE PRISE DE POSITION DE SOCIÉTÉ NUMÉRIQUE

Société Numérique s'oppose à toute mesure de surveillance généralisée en Suisse. L'exemple le plus connu de surveillance généralisée est la conservation de données. Suite à une plainte de notre association, la Cour européenne des droits de l'homme (CEDH) se prononcera prochainement sur la conservation de données en Suisse. Dans ce contexte, Société Numérique préconise le «gel rapide» pour remplacer les pratiques actuelles de conservation systématique des données. En effet, l'alternative dite du «gel rapide» ou «Quick Freeze» des données permet aux autorités d'ordonner l'accès aux données numériques dans le cadre d'investigations tout en préservant les droits fondamentaux.



SOCIETE NUMERIQUE / CH-4000 BALE
OFFICE@DIGITALE-GESELLSCHAFT.CH / SOCIETE-NUMERIQUE.CH

Conservation des données, de quoi parle-t-on?

La conservation des données consiste à collecter et conserver, à titre préventif, les données de communication de tout le monde, sans raison particulière ou soupçon avéré. En Suisse, cette collecte est effectuée par les entreprises de télécommunications comme Salt, Sunrise ou Swisscom, mais aussi par des fournisseurs d'accès Internet qui ont leur siège en Suisse. Les entreprises sont tenues par la «loi fédérale sur la surveillance de la correspondance par poste et télécommunication» (LSCPT) de conserver, pendant six mois, ce que l'on appelle les métadonnées. La police et les ministères publics ainsi que les services de renseignement peuvent utiliser ces données dans le cadre d'enquêtes en Suisse. Les données sont conservées à titre préventif, ce qui signifie que la population en Suisse est soupçonnée par défaut d'être dangereuse ou criminelle.

Ces données, conservées par défaut, montrent qui a communiqué avec qui, quand, où, comment et pendant combien de temps, que ce soit directement ou via l'utilisation d'applications, de services en ligne et de sites web. Les données révèlent ainsi le réseau professionnel et social des personnes recensées et permettent d'établir un profil de déplacement des six derniers mois. Ces données permettent donc d'élaborer des conclusions générales sur le comportement de l'ensemble de la population, et cela même si le contenu des communications lui-même n'est pas enregistré jusqu'à ce jour.

L'objectif officiel des autorités et des politiques est de faciliter l'élucidation des délits. Les mots d'ordre courants sont la «modernisation de la lutte contre la criminalité» et «chances égales face aux criminels».

Pourquoi la conservation des données est-elle illégale et disproportionnée?

La conservation des données est tout simplement une forme de surveillance de masse, car elle touche l'ensemble de la population sans aucun motif ni soupçon. Personne n'en est exempté, ni les avocats, ni les médecins, ni les journalistes. Ainsi, le secret professionnel, comme par exemple celui des avocats ou des médecins, ou la protection des sources des journalistes ne peuvent pas être assurés. Toutes les personnes sont touchées et donc prises dans le filet de la conservation des données.

Dans le même temps, rien ne prouve l'efficacité de la conservation des données. Une étude comparative a démontré, il y a des années déjà, que la conservation des données ne permet pas d'augmenter de façon significative le taux d'élucidation des délits en Suisse. Ce résultat est corroboré par une étude du service scientifique du Parlement européen concernant les taux d'élucidation des délits dans les pays membres de l'Union Européenne (UE).

Par conséquent, la conservation des données constitue une atteinte disproportionnée aux droits humains et en particulier au droit à la vie privée. De nombreuses juridictions suprêmes en Europe, dont la Cour européenne des droits de l'homme (CEDH), ont déjà déclaré la conservation des données inadmissible. Quand la conservation des données doit être autorisée, elle ne l'est qu'à titre exceptionnel et doit se limiter au strict nécessaire. En règle générale, cette pratique est considérée comme illégale et cette lecture doit s'appliquer aux dispositions en vigueur en Suisse, qui concernent tout le monde et prévoient une conservation pendant six mois de toutes les données.

En 2018, Société Numérique a déposé une plainte auprès de la Cour européenne des droits de l'homme (CEDH) concernant la conservation des données en Suisse. Avant cela, nous avions épuisé toutes les voies de recours au niveau national. Société Numérique part du principe que la Cour européenne des droits de l'homme, conformément à sa jurisprudence, déclarera la conservation des données suisse illégale et inadmissible.

Que prévoit la loi suisse sur la protection des données?

La conservation actuelle des données n'est pas conforme avec la loi sur la protection des données (LPD). Selon le principe de la finalité, les données personnelles ne peuvent être collectées et traitées que dans un objectif précis et identifiable par la personne concernée. Dès que cet objectif n'est plus pertinent, les données personnelles doivent être effacées ou anonymisées.

Pour se conformer à la loi LSCPT, les entreprises de télécommunication doivent conserver des données de personnes dont elles n'ont pas besoin pour leur propre activité. Celles des habitants·es de la Suisse pendant six mois, car elles en sont obligées par la loi.

Comment fonctionne la proposition alternative de «gel rapide» («Conservation rapide»)?

Le «gel rapide» est une procédure destiné à conserver les données numériques de personnes soupçonnées. Cette procédure fait partie de la Convention de Budapest[1] du 23 november 2001 comme une première réponse rapide et efficace à la cybercriminalité.

Le «gel rapide», littéralement «Quick Freeze», permet aux autorités de poursuite pénale de faire sauvegarder, à titre préventif, des données numériques qui, pour des raisons légitimes, sont déjà en possession des entreprises concernant des personnes suspectées d'avoir commis un délit.

1. Convention sur la cybercriminalité https://rm.coe.int/168008156d

Dans le cas d'un fournisseur d'accès à Internet, il peut s'agir par exemple de données nécessaires pour garantir la sécurité des données ou pour la facturation. Dans le cas d'un service en ligne, il peut s'agir par exemple de données de géolocalisation que les personnes ont fournies volontairement et de manière éclairée afin de pouvoir utiliser certaines fonctions souhaitées.

En cas d'un soupçon fondé, les autorités de poursuite pénale peuvent désormais interrompre «sur appel» l'effacement ou l'anonymisation de données relatives à des personnes suspectées d'avoir commis un délit, comme l'exige la loi sur la protection des données. Les données doivent, sous certaines conditions, être immédiatement sauvegardées afin de pouvoir être utilisées, le cas échéant, dans le cadre d'une procédure pénale.

Quelles conditions doivent être remplies pour la conservation rapide?

Cependant, le «gel rapide» des données n'est pas sensé être utilisé comme un passe-droit par les autorités de poursuite pénale. Société Numérique exige donc que cette atteinte aux droits fondamentaux des personnes concernées ne soit possible qu'avec une décision judiciaire respectant la transparence dans les procédures judiciaires. La police et le ministère public ne peuvent utiliser les données sauvegardées avec un «gel rapide» que si un tribunal a expressément autorisé leur utilisation dans le cadre d'une procédure conforme à l'État de droit. Le «gel rapide» ne peut être utilisé que par les autorités de poursuite pénale et non par les services de renseignement. Le «gel rapide» doit être réservé aux infractions les plus graves.

Le «gel rapide», en tant que mesure de contrainte, doit faire l'objet de statistiques et être soumis à un contrôle continu de proportionnalité. Une décision judiciaire d'utiliser des données issues d'un «gel rapide» doit être soumise à la transparence dans les procédures judiciaires dès que le secret ne sera plus requis. Toutes les personnes concernées, accusées ou non, doivent être informées dans les plus brefs délais afin de pouvoir protéger leurs droits. Tant que le secret est requis, les intérêts des personnes concernées doivent être défendus devant les tribunaux par un·e avocat·e indépendant·e spécialisé·e dans les droits humains. Un examen public des décisions est nécessaire pour éviter les abus et les contrôles insuffisants.

Pourquoi le «gel rapide» des données est-il une alternative efficace à la conservation des données?

Le «gel rapide» est, sous les conditions mentionnées, une alternative efficace à la conservation des données sans motif et indépendante de tout soupçon. Contrairement à la conservation des données, les données de l'ensemble de la population ne sont pas conservées. Les données disponibles à des fins légitimes sont détruites ou anonymisées conformément à la loi sur la protection des données, à l'exception des conditions de «gel» et d'utilisation à des fins d'application de la loi mentionnées ci-dessus.

Des statistiques antérieures ont montré que la crainte que les autorités chargées de l'application des lois puissent manquer de données numériques essentielles n'était pas fondée. Les délais de conservation typiques des données chez les fournisseurs d'accès à Internet, par exemple, sont souvent de l'ordre de plusieurs semaines, rarement de plusieurs mois.

Le «gel rapide» permet une poursuite pénale efficace tout en renonçant à la conservation des données, qui est contraire aux droits humains. Mais cela n'est valable que si le «gel rapide» est réellement soumis à un contrôle judiciaire et public efficace.

En résumé, Société Numérique constate que:

- La conservation des données en vigueur n'est pas compatible avec les droits fondamentaux et les droits humains.
- Le «gel rapide» permet en revanche une poursuite pénale efficace.
- Le «gel rapide» peut en même temps, sous certaines conditions, préserver les droits fondamentaux et les droits humains.
- Le «gel rapide» pourrait ainsi remplacer la conservation des données, qui est contraire aux droits humains.

En conclusion, Société Numérique demande que:

- La conservation des données soit remplacée en Suisse par le «gel rapide».
- Les conditions mentionnées s'appliquent au «gel rapide».
- Les adaptations correspondantes sont effectuées dans le droit suisse, en particulier dans la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et le Code de procédure pénal (CPP).