Chapitre 4

Tous protégés ?

Les données, produites, contenues dans les ensembles qui constituent le big data, contiennent parfois des informations permettant d'identifier nominativement des individus. Ce sont des données personnelles. Pour limiter la circulation, le commerce, l'échange de ces données, plusieurs solutions existent : c'est ce qui constitue la protection des données personnelles.

Après avoir défini la notion de donné personnelle, nous verrons ce qu'en dit la loi, puis les moyens de protection à la disposition des citoyens. Nous terminerons par l'étude d'une série de reportages radios en rapport avec la question de la protection des données.

4.1 La donnée personnelle, définition légale

En Europe, depuis mai 2018,c'est le RGPD qui défini la notion de donnée personnelle, dans son art. 4. (voir plus bas pour le règlement général sur la protection des données).

> Art. 4. «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

En France, la loi *Informatique et liberté* qui précise la ce qu'est un fichier de donnée.

> Art. 2 « Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique. »

La loi Informatique et liberté : `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460`

Soit : « un nom, un prénom, une photo, une image, une adresse IP».

La loi régit toutes les informations qui permettent d'identifier directement ou indirectement une personne physique.

4.2 Les données sont-elles protégées par le droit ?

4.2.1 Création de la Cnil

En France, en 1974, un projet de fichier permettant d'identifier les citoyens est à l'étude : le projet SAFARI [1]

Ce projet soulève de nombreuses inquiétudes.

De toutes ces critiques et interrogations vont naître :

- La *loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978* [4].
- la Cnil : Commission nationale de l'informatique et des libertés, dont les missions sont définis dans la loi précédente.

C'est le fondement de la protection des données personnelles en France, et l'institution française qui en est chargée.

Tout ce qui constitue un fichier contenant des données personnelles doit être déclaré à la Cnil, sous peine de sanction. Pour une entreprise ou une administration : le moindre fichier informatique contenant un nom est éligible.

La loi est régulièrement mise à jour et modifiée, notamment en quand certaines directives européennes sont transposées en droit français.

Mais d'autres lois touchent les données personnelles.

4.2.2 La loi dite *renseignement*

En 2015, une loi visant à donner davantage de pouvoirs aux services de renseignement est promulguée.

C'est la loi 2015-912 du 24 juillet 2015 relative au renseignement [2]

Les données personnelles sont au cœur de la loi.

Les opposants à la loi notent qu'elle permet :

- l'interception de données personnelles en temps réel sur Internet
- l'extension des pouvoirs de services de renseignement, sans contrôle des citoyens
- la légalisation de pratiques illégales (d'accès aux données) par les services de renseignement
- contrairement aux services web dont le choix d'utilisation (et donc le choix de fournir ou non des données à certains services) est libre, ce n'est pas le cas ici. Tout le monde peut se voir soustraire des données.

4.2.3 Le RGPD : Règlement général sur la protection des données

Le texte est disponible [2].

Le « nouveau » (adopté par le Parlement Européen le 14 avril 2016) règlement général sur la protection des données est entré en vigueur dans toute l'UE le 25 mai 2018. Il remplace une directive de 1995.

Il s'applique à tout organisme collectant et traitant des données concernant ddes citoyens de l'UE, quelque soit son pays d'origine (il est donc applicable à toutes grosses entreprises du Web).

Il introduit de nouveaux droits pour les citoyens, en harmonisant les règles pour tous les pays membres [3] .

Par exemple :

1. Le Monde : `http://rewriting.net/wp-content/le_monde_-_21_03_1974_009-3.jpg`
2. Voir [5] `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899`.

– Consentement écrit pour recueillir les données (c'est ce qui apparaît sur tous les site Web)
– le droit à l'oubli numérique
– la portabilité des données (par exemple pour passer d'un réseau social à l'autre). Un réseau doit être en mesure de fournir la totalité des données d'un utilisateur, dans un format utilisable (voir la question de la qualité des données, et le droit d'accès à ses données)
– le droit d'être informé en cas de piratage des données
– la possibilité d'actions de groupe pour des questions de données

Toutes les entreprises (dont les Gafa) ont été obligées de s'y conformer. Des sanction ont déjà été appliquées.

4.3 Réclamer ses données ?

La protection des données, c'est également la possibilité de savoir qui détient quelles données nous concernant. La loi impose à tout détenteur de données personnelles de laisser l'accès à ses données, aux personnes concernées. Tout le monde peut donc demander ses données et est en droit d'en connaître les méthodes et procédures de réutilisation.

4.3.1 À qui demander ses données ?

A tout le monde !

Par exemple [3] :

– assurances maladie (actuelle et ancienne)
– assurance domestique, voiture ...
– tous ceux qui utilisent la vidéo-surveillance
– hôpitaux (dossier médical)
– chaîne de vente de textiles
– Facebook, ...
– banques
– agences immobilières
– grande distribution
– Amazon
– Google
– Samsung
– écoles, universités,...
– éditeurs d'apps mobiles
– Microsoft (pour Windows)
– opérateurs mobiles
– EDF, société de distribution de l'eau,...
– ... ...

La Cnil propose des exemples de courrier de demandes d'accès (et de rectification ...) : `https://www.cnil.fr/fr/modeles/courrier`

Je ne peux vous conseiller de demandr vous même vos propre données à ddes entreprises, administrations,... et d'en analyser le résultat !

3. Liste inspirée de [6].

4.3.2 Que trouve-t-on dans les réponses ?

C'est extrêmement variable ! Certaines entreprises jouent le jeu, d'autres pas du tout ! Parfois les envois sont numériques (ou sur CD, clefs USB) dans des formats difficiles à lire.

Comment être sûr qu'il ne manque rien ? Voir par exemple le cas d'Amazon et son envoie initial très incomplet à l'équipe d'*On en Parle* : [7].

4.4 Quelle protection ?

Avoir accès à ses données c'est une forme de protection. Mais elle n'est pas forcément suffisante. Il faut parfois recourir à des moyens techniques ou organisationnels : partager uniquement ce que l'on souhaite, ou tenter de bloquer l'accès aux données.

4.4.1 Reprendre la main ? La question des « self data »

Il s'agit là de permettre à des citoyens de partager d'eux-mêmes leurs données. Quelques exemples (en Suisses dans les exemples suivants).

4.4.1.1 L'exemple d'*healthbank* et les données médicales

Web : `https://www.healthbank.coop`.

Ici, le patient dépose ses données sur la plate-forme. Il partage ses données uniquement aux services qu'il choisi. Par exemple : son médecin, des labo etc. Ou avec... personne ! Les participants (pour certains partages) peuvent être rémunérés.

4.4.1.2 Encore des données de santé : Midata

Web : `https://www.midata.coop`

Ce site permet de déposer ses données, par exemple dans le cadre d'un test clinique de médicament. Là aussi, tout se fait de manière volontaire. Il n'y a pas de "pompe à données" qui tenterait de récupérer des données de manière inappropriée.

Un intérêt pour la gestion et les tests dans le cadre du Covid-19 ?

Le self-data est une nouvelle manière de gérer les données personnelles. Mais il n'y a que très peu de recule sur ces initiatives. Qu'en sera-t-il à long terme ? À qui appartiendra le site ? Les données ? Risquent elles d'être monétisées ? Est-ce réellement une moyen de protéger ses données ?

Plus d'infos sur les principes du *selfdata* sur : `http://mesinfos.fing.org/selfdata/`

4.4.2 La question du chiffrement

Des données qui transitent, ou sont stockées sans moyen technique de protection sont très vulnérables. Sans protection adaptée, il est relativement simple pour des individus maîtrisant les aspects techniques, d'accéder à des machines (serveurs, téléphones...) qui stockent ou font transiter des données. Le moyen utilisé pour protéger ces informations est le chiffrement. Les données, les conversations, les fichiers vont subir une transformation qui vont les rendre illisibles. Pour y accéder il faudra disposer du code utilisé pour transformer

les données. On va ensuite fait dans subir le même traitement aux données, dans le sens inverse. C'est la *clef de chiffrement*.

4.4.2.1 Enjeux et principes

Chiffrement des machines et des communications.

Le chiffrement limite les actions d'individus malveillants, de force de répressions (et de renseignement) et participe ainsi au soutien de la démocratie (voir par exemple le rôle de certains outils de communication dans divers cas de révoltes et manifestations...).

Mais diverses « campagnes » contre l'utilisation du chiffrement (par les états notamment) ont été menées, notamment en utilisant les arguments de lutte contre le terrorisme.

Mais pour les utilisateurs, il est facile de protéger ses données. Il s'agit, par exemple, d'utiliser les outils adaptés, qui chiffrent eux-mêmes les données. Ils sont souvent très accessibles. Par exemple :

- WhatsApp (mais c'est plus compliqué que ça dans ce cas là),
- SSL (chiffrement des données sur le Web, utilisation transparente pour l'utilisateur. C'est le S de `https://`,
- Telegram ou Signal
- Protonmail, plutôt que Gmail
- ...

Pour les gouvernements, le chiffrement reste contrôlable quand les entreprises (les fournisseurs d'accès à Internet...) le mettent en place. Il est possible d'exercer diverses pressions sur ces entreprises pour accéder néanmoins au données.

Mais c'est beaucoup plus compliqué quand ce sont les individus eux-mêmes qui protègent leurs données.

À terme, avec le chiffrement, il sera beaucoup plus compliqué de faire de l'espionnage de masse (par exemple avec les IMSI-catchers qui permettent d'intercepter les communications téléphones portables etc.). Mais les services de renseignement ont toujours un (ou des !) coup d'avance.

4.4.2.2 Quels problèmes ?

Quelques inconvénients du chiffrement [4].

- temps de calcul allongé (donc temps d'accès aux données allongé)
- difficulté pour un moteur de recherche d'accéder à des données chiffrées
- chiffrement pour un temps donné seulement : il faut rallonger la clef de chiffrement en même temps que les puissances des machines augmentent et que les recherche en cryptographie progressent : plus la clef est simple plus elle est rapide à déchiffrer ; plus l'ordinateur est puissant, plus il ira vite...

4.5 Une mise en application : l'enquête ouverte #Mes-données

Entre 2015 et 2017, des journalistes de la Radio Télévision Suisse ont menée une *enquête ouverte*. À travers l'émission *On en parle* (sur la chaîne La Première (L-V, 8h30-

4. Voir dans [1] p. 9. par. 36.

9h30)) ils ont lancé une enquête participative sur l'ensemble de la question de la protection des données.

L'idée était d'enquêter sur l'ensemble de ce qui touche à la question des données personnelles, en mettant les auditeurs à contribution, notamment en utilisant un groupe Facebook [8].

Des points très réguliers étaient faits dans l'émission. Tous les traitements journalistiques sont disponibles sur `http://www.rts.ch/mesdonnees`.

Les éléments qui suivent sont extraits de cette enquête. Ils servent ici d'illustration et de « cas pratiques » concernant la question de la protection.

Pourquoi étudier des exemples suisses ? Parce qu'aucune enquête équivalente ne s'est déroulée en France. Il existe des éléments d'informations français, mais ils ne sont pas, à ce point, exhaustifs ni disponibles. Ensuite car les résultats sont techniquement très facile d' accès (et c'est important pour un enseignement). Enfin, car même si la règlementation n'est pas la même, les principes le sont. De plus, le RGPD, qui est européen (donc en théorie non applicable en Suisse) impacte de nombreuses entreprises en Suisse, qui applique de fait, largement le texte.

Les liens, cliquables, sont dans la page HTML de consignes !

4.5.1 Présentation de l'enquête en vidéo

Vidéo de juin 2015, lancement de l'enquête ouverte, participative.
`https://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-155`

4.5.2 Video de la 5e réunion

Les réunions étaient hebdomadaire. Après la 5ème séance.
`https://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-155`

4.5.3 Au bout de 100 j d'enquêtes

Le point en octobre 2015 :
`https://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-155`

4.5.4 L'avis du préposé fédéral à la protection des données

En janvier 2016. Satifaisant, sans plus !
`http://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-25+janvier+2016`

4.5.5 Tout reste ouvert

Synthèse (audio) en mai 2016, des éléments de l'enquête. Il reste beaucoup de travail !
`http://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-Donnes+donn\%C3\%A9es\%3A+tout+reste+ouvert\%21`

Bibliographie

[1] Dominique Carré andJacques Vétois, *Contrôle social et techniques numériques. approche sociohistorique*, tic&société **10** (2016), no. 1, URL `http://ticetsociete.revues.org/1973`.

[2] Eur-Lex, *Règlement (ue) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ce (règlement général sur la protection des données) (texte présentant de l'intérêt pour l'eee)*, 2016, [En ligne ; Page disponible le 23 mars 2018], URL `http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1522075637751&uri=CELEX:32016R0679`.

[3] Julien Lausson, *Rgpd : 10 questions pour comprendre le nouveau règlement sur la protection des données*, Numerama (2018), URL `https://www.numerama.com/politique/329191-rgpd-tout-savoir-sur-le-reglement-sur-la-protection-des-donnees-si-vous-et` `html`.

[4] Legifrance, *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, 1978, [En ligne ; Page disponible le 23 mars 2017], URL `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460`.

[5] ———, *Loi nº 2015-912 du 24 juillet 2015 relative au renseignement*, 2015, [En ligne ; Page disponible le 23 mars 2017], URL `https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899`.

[6] On En Parle, *A qui demander des données ?*, 2015, URL `https://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-1559897573758`.

[7] ———, *Amazon s'excuse*, 2016, URL `https://www.rts.ch/la-1ere/programmes/on-en-parle/6813759.html#timeline-anchor-1559897573789`.

[8] Radio Télévision Suisse, *Enquête ouverte : #mesdonnées*, 2015, [En ligne, le 04-11-2015], URL `\url{https://www.facebook.com/groups/mesdonnees/}`.