Aspect Juridique
(Licence 2)
(MI)

Pr. Ghalem BELALEM
Université Oran1 Ahmed Ben Bella
Ghalem1dz@yahoo.fr

Chapitre 2 :

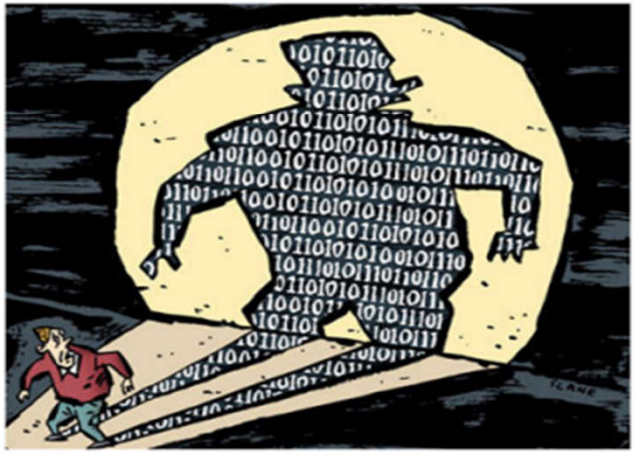
Données personnelles et la vie privée!

Plan :

1. **Introduction et définition**
2. **Exemples**
3. **Données sensibles**
4. **Le respect de la vie privée**
5. **Vie privée et Informatique**
6. **Loi en Algérie**
7. **RGPD en Europe et en Afrique**
8. **Quelques sanctions**
9. **Négligences**
10. **Conclusion**

Internet!

Sur Internet, chaque personne laisse des traces numériques reliées à son identité.



« RIEN NE S'EFFACE SUR INTERNET»

Introduction et Définition

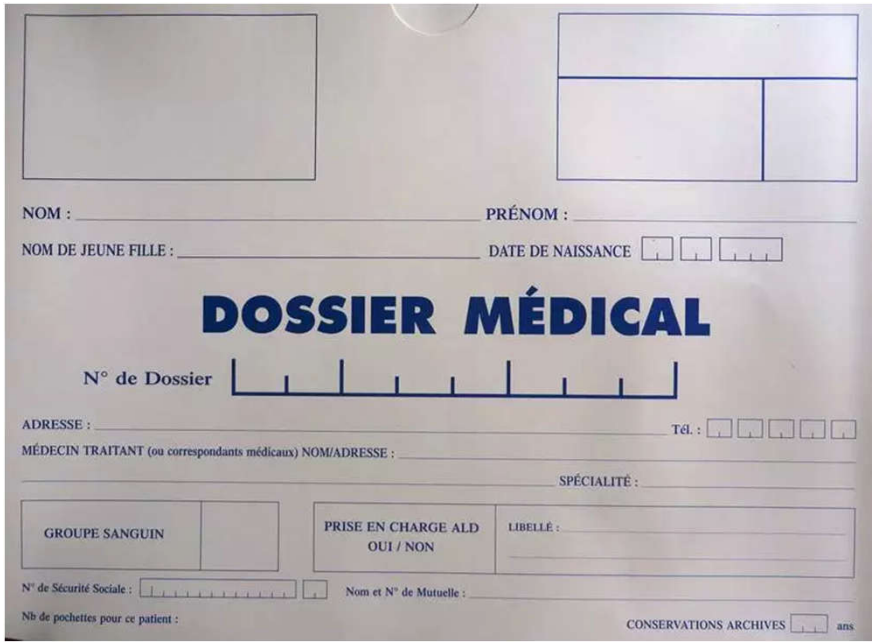
Donnée personnelle

Toute information identifiant **directement** ou **indirectement** une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Introduction et Définition

Lorsque l'on parle d'accès direct à une donnée à caractère personnel :

Cela veut dire l'accès à la fiche de renseignement complète du citoyen sur une base de données ou un document papier contenant toutes les informations précises d'identification.



Par exemple :

- Une fiche client
- Une fiche de paye
- Un dossier médical
- Une facture ou un devis
- Tout document papier ou élément d'une base de données électronique qui rassemblerait des éléments permettant d'identifier un individu.

Introduction et Définition

Lorsque l'on parle d'accès indirect à une données à caractère personnel :

On veut dire, l'accès à une donnée qui permettrait d'identifier un citoyen européen en la croisant avec d'autres sources de données.

Par exemple :

- Un numéro de téléphone permet de retrouver le nom et l'adresse d'un citoyen, par le biais d'un annuaire téléphonique.

- Une plaque d'immatriculation permet de trouver le nom et l'adresse d'un citoyen, par le biais du fichier des cartes grises.

- Le numéro de sécurité sociale permet de retrouver les coordonnées et le dossier médical du citoyen par le biais du fichier de la sécurité sociale.

Exemples

Exemples de données à caractère personnel :

- Un nom, un prénom, une photo, sont des données à caractère personnel que l'on trouve par exemple sur des badges d'accès au sein de votre entreprise.

- Une adresse mail qui peut-être utilisée sur un simple moteur de recherche pour retrouver la personne concernée.

- Un numéro de téléphone. il suffit d'un annuaire téléphonique pour retrouver les informations sur le citoyen.

- Un CV, une candidature, que vous recevez tous les jours par la poste. Si vous les laissez traîner dans votre bureau ou sur le comptoir de votre magasin, ce sont des données directement accessibles à tous.

- Une fiche de paye d'un employé contient énormément de données à caractère personnel.

- Des images de vidéosurveillance:

  Elles sont soumises au règlement général sur la protection des données, et doivent être protégées au même titre que les informations personnelles de vos employés.

- Un numéro de sécurité sociale de patient par exemple, pourrait donner accès à un dossier médical. Dans ce cas on parle de **données très sensible**.

- Une plaque d'immatriculation qui permet de remonter au nom et à l'adresse du titulaire de la carte grise.

- Une adresse IP, que l'on enregistre sur les serveur lors de la connexion de votre site internet. Cette donnée permet de remonter jusqu'à l'adresse de l'utilisateur en passant par le fichier de l'opérateur.

- … beaucoup d'autres…

Données sensibles

Données Sensibles

Ce sont les informations qui révèlent la prétendue origine **raciale** ou **ethnique**, les **opinions politiques**, les **convictions religieuses** ou **philosophiques** ou l'**appartenance syndicale**.

Ce sont également les **données génétiques**, les **données biométriques** aux fins d'identifier une personne physique de manière unique.

Il est interdit de recueillir et d'utiliser ces données. Sauf dans certains cas précis et notamment :

- Si la personne concernée a donné son **consentement exprès** (écrit, clair et explicite) ;
- Si ces données sont nécessaires dans un **but médical** ou pour la recherche dans le domaine de la santé;
- Si leur utilisation est justifié par l'**intérêt public et** autorisé par **une instance judiciaire** ;
- Si elles concernent les **membres ou adhérents d'une association** ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Le traitement de ces données doit considérer un niveau de sécurité supplémentaire.

Le respect de la vie privée

« Le droit d'une personne de contrôler l'accès à sa personne et aux renseignement qui la concerne. Le droit à la vie privée signifie que la personne décide des renseignements qui sont divulgués, à qui et à quelles fins. »

Une **atteinte à la vie privée** suppose l'accès **non autorisé** à des renseignements personnels ou la collecte, l'utilisation ou la communication non autorisée de tels renseignements.
Certains des cas d'atteinte à la vie privée surviennent lorsque des renseignements personnels sont **volés**, **perdus** ou **communiqués par erreur**.

Vie privée et informatique

L'apparition de l'informatique a changé la nature des problèmes posés par la notion de vie privée.

Si l'informatisation des données a été généralement considérée comme un progrès, elle s'est aussi accompagnée de dangers liés à la possibilité pour une entité d'avoir un accès non contrôlé aux informations de nombreux citoyens.

Généralement, la protection de la vie privée repose sur la mise en place de moyens légaux (par exemple loi informatique et libertés), techniques (cryptographie) ou organisationnels (règles internes).

Vie privée et Internet

La protection des données personnelles et de la vie privée à l'ère des réseaux sociaux comme Facebook et Twitter, des smartphones et des objets connectés devient un défi pour les utilisateurs comme pour les organismes chargés d'encadrer ces évolutions.

Mais la maîtrise de ses propres données passe d'abord par une **sensibilisation** ou une **connaissance** de ce risque comme des outils pour se protéger d'un vol par exemple. Parmi eux, le chiffrement permet d'empêcher la lecture de ses fichiers par une tierce personne.

Vie privée et informatique

«Votre écran d'ordinateur n'est pas un mur derrière lequel vous vous cachez, mais plutôt une fenêtre grande ouverte par laquelle deux milliards d'inconnus vous observent. »

Jean Chartier, Président de la Commission d'accès à l'information du Québec

(28 janvier 2011 la journée mondiale de la protection de la vie privée)

La Loi de protection en Algérie

La Loi sur la protection des personnes physiques dans le traitement des données personnelles est entrée en vigueur.

Les détails du texte sont énoncés dans le journal officiel paru ce mardi 3 juillet. C'est l'Article 3, de cette Loi portant n° **18-07 du 10 juin 2018**, qui définie les « Données à caractère personnel ».

Ainsi, il s'agit, selon le texte, de toute information, quel qu'en soit son support, concernant une personne dont les données à caractère personnel font l'objet d'un traitement.

Art. 55. — Quiconque procède à un traitement de données à caractère personnel, en violation des dispositions de l'article 7 de la présente loi, est puni d'un emprisonnement d'un (1) an à trois (3) ans et d'une amende de 100.000 DA à 300.000 DA.

Art. 57. — Est puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 200.000 DA à 500.000 DA, quiconque procède, sans le consentement exprès de la personne concernée et hors les cas prévus par la présente loi, aux traitements des données sensibles.

Art. 56. — Est puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 200.000 DA à 500.000 DA, quiconque procède ou fait procéder à des traitements de données à caractère personnel sans respect des conditions prévues par l'article 12 de la présente loi.

Art. 58. — Est puni d'un emprisonnement de six (6) mois à un (1) an et d'une amende de 60.000 DA à 100.000 DA ou de l'une de ces deux peines seulement, quiconque met en œuvre un traitement des données ou utilise celles-ci à des fins autres que celles pour lesquelles elles ont été déclarées ou autorisées.

https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/107253/131953/F519624415/DZA-107253.pdf

RGPD! Règlement Général sur la Protection des Données

Le RGPD pour Règlement Général sur la Protection des Données est un texte de loi européen adopté en avril 2016. Ce texte de référence européen porte sur la protection des données à caractère personnel. .

Si le RGPD tend à protéger la vie privée des internautes européens, elle a des répercussions très fortes sur les professionnels et les entreprises qui collectent des données.

Les objectifs du RGDP

Redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des entreprises

Il existe 3 objectifs du RGPD :

1. Renforcement du droit des citoyens majeurs et mineurs;
2. Responsabilisation des acteurs de la donnée (entreprises et intermédiaires);
3. Renforcement du contrôle et application des sanctions sur tout le territoire européen.

RGPD! Règlement Général sur la Protection des Données

Les conséquences

Le Règlement Général sur la Protection des Données a bouleversé ou va bouleverser le fonctionnement de **certaines entreprises**. Ces dernières ont vite compris qu'elles doivent mettre en place des modifications sur leur fonctionnement avant le **25 mai 2018**, date d'entrée en vigueur.

Identifier les traitements des données personnelles

Les entreprises doivent être capables de garantir et de prouver que le traitement des données est conforme et sécurisé à tout moment.
Le traitement des données doit pouvoir être traçable pour justifier de la mise en place de bonnes pratiques en termes de manipulation des données personnelles (collecte, stockage, utilisation, partage ou destruction).

Étendre les obligations aux sous-traitants

Les sous-traitants doivent aussi se mettre en conformité et les entreprises doivent choisir un prestataire qui répond aux exigences de la nouvelle réglementation.

RGPD! Règlement Général sur la Protection des Données

Donner de nouveaux droits aux personnes

Le RGPD donne de **nouveaux droits** aux personnes sur l'utilisation et le traitement des données personnelles.

- Le droit à la portabilité des données : prévoit que les personnes peuvent recevoir les données qui les concernent et qui ont été transmises à un organisme et que les personnes puissent aussi **les transmettre à un autre organisme sans restriction**. Ce transfert doit se faire « dans un format structuré, couramment utilisé et lisible par machine ».

- Le droit à l'oubli : permet à une personne de demander la **destruction des données personnelles** qui la concernent.

- Le droit sur la protection des données des mineurs de moins de 16 ans oblige les organismes à recevoir **un accord d'un représentant légal** pour collecter des données sur le jeune public.

RGPD! Règlement Général sur la Protection des Données

Le rôle de la CNIL

La Commission nationale de l'informatique et des libertés (CNIL) est l'autorité chargée du contrôle des RGPD et de veiller au respect et à l'application conforme du RGPD. Le RGPD suit pour cela une logique de contrôle.

Quelques sanctions

Il faut noter que la responsabilité d'une entreprise s'étend aux fichiers partagés avec ses fournisseurs.

- Le groupe Darty a écopé d'une amende de 100.000 euros en juillet 2018 en raison d'un formulaire de service après-vente créé par un prestataire externe et insuffisamment protégé.

- Hertz, amende de 40.000 euros (juin 2018).
- Optical Center, amende de 250.000 euros (juin 2018).
- Daily Motion, amende de 50.000 euros (août 2018).
- …

Enfin, dans le pire des cas, l'entreprise qui ne se conforme pas au RGPD encourt soit une sanction pécuniaire à hauteur de **2%** à 4% de son chiffre d'affaires annuel mondial, soit encore des sanctions pénales de **5 ans** d'emprisonnement ou **30 000 euros** d'amende.

Quelques sanctions

Il faut noter que la responsabilité d'une entreprise s'étend aux fichiers partagés avec ses fournisseurs.

- Le groupe Darty a écopé d'une amende de 100.000 euros en juillet 2018 en raison d'un formulaire de service après-vente créé par un prestataire externe et insuffisamment protégé.

- Hertz, amende de 40.000 euros (juin 2018).
- Optical Center, amende de 250.000 euros (juin 2018).
- Daily Motion, amende de 50.000 euros (août 2018).
- …

Enfin, dans le pire des cas, l'entreprise qui ne se conforme pas au RGPD encourt soit une sanction pécuniaire à hauteur de **2%** à 4% de son chiffre d'affaires annuel mondial, soit encore des sanctions pénales de **5 ans** d'emprisonnement ou **30 000 euros** d'amende.

Et en Afrique!

Pendant que, de plus en plus la protection de la vie privée et des données personnelles devient un enjeu stratégique partout dans monde, l'Afrique semble encore **ne pas saisir son importance**.

On se rappelle du scandale Facebook – cabinet londonien **Cambridge Analytica** qui a occasionné la fuite et l'exploitation à des fins politiques de données personnelles de **80 millions** d'utilisateurs du réseau social !!

Alors que les parlements des Etats-Unis d'Amérique et de l'Union Européens ont convoqué Mark Zuckerberg, Fondateur de Facebook pour s'expliquer sur cette situation quelque peu **gênante**, les pays africains sont **restés silencieux**. **Manque de vision**, **manque de courage ou simple ignorance** ?

Malheureusement ce que ces dirigeants ignorent, c'est qu'à l'heure du **Big Data** et de l'**Intelligence Artificielle** **(IA)**, **les données personnelles et la vie privée des Internautes** ont plus de valeurs que les minéraux les plus rares des sous-sols Africains

L'espoir est donc permis que les états africains prennent le train déjà en marche de la sécurisation et de la protection de la vie privée de leurs concitoyens.

https://www.cpaiinc.com/2018/07/12/enjeux-de-protection-donnees-personnelles-de-vie-privee-afrique/

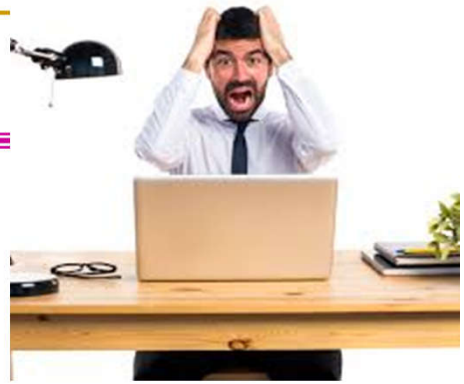
Exemple!

La mise en ligne d'un « faux profil » portant le nom et le prénom d'une personne existante, ainsi que des photos de cette personne et des anecdotes sur sa vie personnelle, constitue une **atteinte à son droit au respect de la vie privée** et à son droit à l'image.

Dans cette affaire, une personne avait créé un profil Facebook pour une personnalité connue et les utilisateurs de Facebook pouvaient légitimement croire s'adresser directement à cette personnalité. L'auteur de la supercherie a été condamné à la somme totale de 1 500 euros (500 euros pour l'atteinte à la vie privée et 1 000 euros pour la violation du droit à l'image), à titre de dommages et intérêts en réparation du préjudice en résultant, ainsi que la somme de 1 500 euros pour les frais de procédure.

Dans une autre affaire, un site internet avait publié la photo d'une actrice française avec son jeune fils sans le consentement de celle-ci. Le site a été condamné à 1 500 euros pour atteinte à la vie privée et à l'image de l'actrice. Il a été précisé que le fait que cette photo ait déjà été publiée sur d'autres sites n'est pas une excuse.

Négligeance!



Negligeance des internautes

Pire ennemi: soi-même

- En divulguant trop d'informations sur soi (photos, histoire de notre vie, etc.).
- En faisant confiance facilement aux autres.
- En affichant des informations sensibles : la date de naissance, le numéro de téléphone, le lieu de travail, l'emplacement géographique, etc.
- En se comportant d'une façon émotionnelle:
  - La curiosité nous incite parfois à cliquer sur des liens malveillants.
  - La compassion peut nous pousser à envoyer de l'argent à un ami présumé qui prétend être victime de vol.
  - Etc.

Conclusion

Astuce

Il faut s'abstenir de toute diffusion de contenus ou d'informations relatives à la vie privée des autres sans leur autorisation.

Même lorsqu'il s'agit de sa propre vie privée, il convient d'être attentif avant de publier un contenu sur le web.

Il peut s'avérer intéressant de surveiller ce que l'on dit de soi sur internet et parfois de nettoyer les informations considérées comme obsolètes ou critiques (cette notion est expliquée dans la fiche « Le droit à l'oubli »).

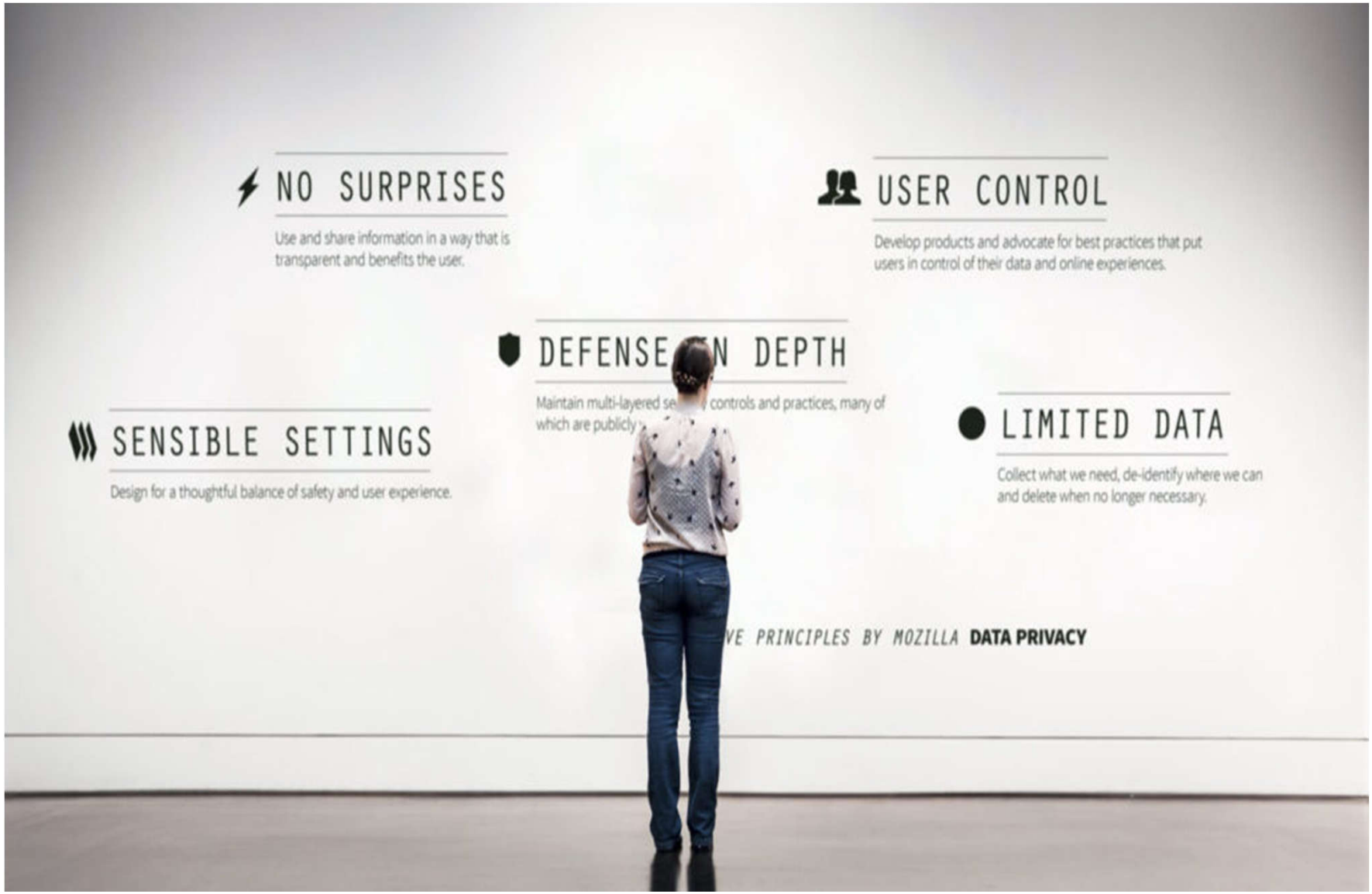
Astuce

Il convient donc de temps à autre de contrôler le Web par des moyens aussi efficaces et rapides que de saisir son propre nom ou pseudo pour voir s'il est réutilisé par un tiers ou non. On peut aussi utiliser les solutions d'alerte automatique des moteurs de recherche.

Merci pour votre attention

Vos Questions !!!

Discussions …


NO SURPRISES
Use and share information in a way that is transparent and benefits the user.
USER CONTROL
Develop products and advocate for best practices that put users in control of their data and online experiences.
DEFENSE IN DEPTH
Maintain multi-layered
controls and practices, many of
which are publicly
SENSIBLE SETTINGS
Design for a thoughtful balance of safety and user experience.
LIMITED DATA
Collect what we need, de-identify where we can and delete when no longer necessary.
VE PRINCIPLES BY MOZILLA DATA PRIVACY