



UNIVERSITÉ PARIS 1

**PANTHÉON SORBONNE**

---



UNIVERSITÉ PARIS 1  
**PANTHÉON SORBONNE**



## 2.4 S'insérer dans un monde numérique

# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- RGPD
- La dématérialisation des services publics
- Modèles et stratégies économiques

# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- RGPD
- La dématérialisation des services publics
- Modèles et stratégies économiques

# Identification et e-reputation: Authentification

- L'authentification est la procédure qui permet à un système informatique de vérifier l'identité de l'utilisateur, afin d'autoriser l'accès à un espace et/ou des ressources en accès réservé.
- Les bonnes pratiques :
  - garder votre mot de passe **secret** ;
  - choisir un mot de passe **complexe** composé d'au moins **8** lettres et chiffres, de minuscules et de majuscules, évitez les noms communs ;
  - éviter de choisir le même mot de passe pour plusieurs comptes.
  - se prémunir d'une usurpation d'identité :
    - ne jamais mémoriser votre mot de passe sur un ordinateur que vous n'êtes pas le seul à utiliser !
    - savoir reconnaître les tentatives de hameçonnage ou **phishing** :
      - Le phishing consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, voire relations etc. — afin d'obtenir des renseignements personnels. (exemple : vous recevez un faux courriel de votre banque, d'EDF ou d'e-bay)

# Identification et e-reputation: Bien choisir son nom de domaine

- Pour créer un site web il est nécessaire de déposer un nom de domaine auprès d'un **bureau d'enregistrement (Registrar)** ;
- Ce nom doit être pertinent et stratégique à l'image du nom d'une marque car il est porteur de sens et contribuera à mettre en avant une idée et/ou l'identité de son propriétaire sur internet ;
- L'enregistrement d'un nom de domaine permet de se protéger d'un « vol » éventuel par une concurrence potentielle. Il permet également d'obtenir une **adresse email personnalisée** et d'éviter que le nom de la plateforme utilisée pour la création du site apparaisse dans l'url ;
- Il est nécessaire de le **renouveler avant son expiration**, celui-ci n'étant pas déposé à vie ;
- Il est possible depuis peu de choisir quelques extensions géographiques françaises pour son nom de domaine : paris, .bzh, .corsica et .alsace.

Ex : [www.bienvenue.paris](http://www.bienvenue.paris)

# Identification et e-reputation: Votre identité sur le web

- Éléments de votre identité numérique :
  - vos coordonnées : adresse, e-mail, téléphone ;
  - l'adresse IP de votre ordinateur qui permet de vous localiser ;
  - les moyens d'expressions que vous utilisez laissent des traces : les blogs, les podcasts ;
  - les contenus que vous partagez via des outils de publication (Facebook, Twitter, You Tube, Snapchat...) : photos, vidéos, musique, liens ;
  - quand vous donnez votre avis sur un produit, un service, une prestation ;
  - vos hobbies participent également à votre image sur le web, que vous soyez passionnés de musique, de cuisine, de saut en parachute, vous communiquez sur les réseaux de passionnés ;
  - tous vos achats en ligne donnent des indices sur vous-mêmes ;
  - sur les portails et réseaux sociaux professionnels, vous donnez des informations sur vous ;
  - les sites de rencontre, les jeux en lignes et les mondes virtuels où vous affichez votre avatar donnent aussi des éléments sur vous.

# Identification et e-reputation: La e-reputation

- La e-reputation est votre image sur le web
- Des informations vous concernant peuvent être publiées sur le web :
  - par vous-même ;
    - en remplissant un formulaire, en signant une pétition, en participant à un forum et même juste en navigant sur le web ;
  - par des connaissances, des collègues, des amis, etc ;
  - par des institutions.
- L'utilisation d'un pseudo est parfois suggérée par un fournisseur de service. En limitant le lien entre votre identité réelle et l'identité numérique (ou les identités choisies) vous vous protégez.
- Il faut bien distinguer deux choses : les traces qui composent votre identité numérique privée et celles qui composent votre identité numérique professionnelle :
  - ne jamais mélanger les deux sans le vouloir.
  - ne mélangez pas les contextes en communiquant, par exemple, sur votre réseau professionnel avec le nom de votre avatar dans un jeu en ligne.



# Identification et e-reputation: Les dangers des RS

- Les dangers des réseaux sociaux :
  - Les réseaux sociaux proposent des fonctionnalités permettant de publier des photos et des informations sur soi (croyances, opinions politiques, photos privés) ou sur un tiers, ce qui peut représenter une atteinte au droit à l'image, à la vie privée :
    - Les employeurs font une recherche internet sur les personnes qu'ils sont susceptibles de recruter.
    - Des études ont montré qu'à travers les publications sur les réseaux sociaux et le partage d'informations il est possible de connaître les opinions politiques, les goûts et même l'orientation sexuelle d'une personne.

# Votre identité sur le web : Moteurs de recherche

- **Méfiez-vous des moteurs de recherche.**
- Un moteur de recherche parcourt toutes les pages du web en accès public et les recense :
  - en récupérant les mots clés de la page ;
  - en gardant dans le cache une copie de cette page . Vous croyez avoir supprimé l'information mais elle reste dans le cache du navigateur.
- Exemples d'informations indexées par les moteurs de recherche :
  - toute intervention dans un forum public ;
  - toutes les informations avec un profil public dans Facebook ;
  - tous les textes, photos et commentaires d'un blog ou d'un site public ;
  - et bien d'autres informations !

**Remarque** : Il est possible de retrouver le contenu de sites web supprimées. En effet, certaines organisations réalisent des clichés instantanés de tous les sites Internet. Grâce à des technologies modernes, ces organisations recueillent des clichés de façon continue et les mettent gratuitement à disposition sur Internet (Ex : Wayback Machine du projet Internet Archive).

# Votre identité sur le web : bonnes pratiques

- Les bonnes pratiques pour préserver votre e-réputation :
  - ne jamais publier d'informations personnelles sur un site en accès libre, sur son blog, sur son mur Facebook, etc.
    - vérifiez le paramétrage de votre profil sur Facebook (options de confidentialité). Vous pouvez paramétrer l'accès aux informations, en contrôlant la partie publique (accessibles par tous et pouvant être référencées par les moteurs de recherche) et la partie à accès restreint (privée), réservée à vos relations. Vous êtes ainsi en mesure de protéger les informations pouvant vous nuire.
  - ne pas publier d'informations sur un ami, un collègue, ni poster des photos de lui sans son accord ;
  - demander un droit de rectification aux sites qui diffusent une mauvaise image de vous ;
  - soyez vigilants sur le marquage de photos dans Facebook. Souvent, il s'effectue à votre insu.

# Identification et e-reputation: Vos traces locales

- Grâce au site de la CNIL (Commission Nationale de l'Informatique et des Libertés), découvrez ce que tout serveur peut récupérer comme information sur votre ordinateur, ce qu'il peut collecter comme données sur votre navigation et vos saisies au clavier :
  - <http://www.cnil.fr/vos-droits/vos-traces>
- Une simple navigation sur le web enregistre sur votre disque dur :
  - la liste des URL consultées (historique de navigation) ;
  - les données saisies (historique des recherches et formulaires) ;
  - les fichiers que le navigateur télécharge pour afficher les pages web (cache du navigateur) ;
  - les fichiers que vous avez téléchargés (téléchargements).
- Les bonnes pratiques :
  - effacer l'historique de navigation, des téléchargements, etc. à chaque fois que vous fermez votre navigateur. Vous pouvez aussi utiliser la « navigation privée » ;
  - paramétrer votre navigateur pour que ces informations soient automatiquement effacées.

# Identification et e-reputation: Cookies

- Une simple navigation sur le web enregistre aussi sur votre disque dur des **cookies** :
  - ce sont des témoins de connexion prenant la forme d'un fichier texte ;
  - ils ne doivent pas être confondus avec des logiciels espions ou des virus ;
  - ils peuvent être utilisés pour maintenir les données relatives à l'utilisateur durant sa navigation, mais aussi à travers plusieurs visites ;
  - ils peuvent être utilisés pour mémoriser l'information sur l'utilisateur d'un site, dans le but de lui montrer un contenu approprié dans le futur ;
  - les cookies de pistage sont utilisés pour suivre les habitudes de navigation des utilisateurs d'internet ;
  - ils peuvent être interceptés, volés, modifiés...
- **Les bonnes pratiques** :
  - toujours fermer toutes les fenêtres de votre navigateur afin que les cookies d'identification soient effacés ;
  - il est toujours possible de supprimer partiellement ou totalement les autres cookies dans les options du navigateur.

# Identification et e-reputation: Vos traces sur internet

- Quand vous consultez une page web, votre navigateur interroge le serveur web hébergeant cette page pour y récupérer les données (textes, images, ...) à télécharger.
  - Cette requête envoie des variables caractérisant votre environnement :
    - votre **adresse IP** ;
    - votre **nom d'hôte** (ou fournisseur d'accès) ;
    - votre **système d'exploitation** ;
    - la version de votre **navigateur**.
  - Le serveur web visité peut garder ces traces et suivre ainsi votre navigation sur son site !
    - Ex : Si vous avez visité le site d'Amazon, il vous propose à la visite suivante des produits qui peuvent correspondre à vos besoins car le serveur a gardé en mémoire les pages que vous avez consultées.
- Pour échapper au ciblage publicitaire, une sociologue américaine a veillé à ne laisser aucune trace de sa grossesse sur Internet mais aussi dans ses paiements en carte de crédit mais cette expérience très contraignante l'a rendu suspecte pour les autorités américaines.

# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- RGPD
- La dématérialisation des services publics
- Modèles et stratégies économiques

# Informatique et liberté: CNIL

- La loi informatique et libertés du 6 janvier 1978 encadre le traitement des **données à caractère personnel** :
  - la Commission Nationale de l'Informatique et des Libertés ([CNIL](#)) en assure le respect ;
  - elle est fondée sur le principe que « l'informatique doit être au service de chaque citoyen » et qu'elle « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Article 1<sup>er</sup>, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.





# Informatique et liberté: CIL et obligations

- Un Correspondant Informatique & Libertés (CIL) :
  - est désigné dans l'entreprise pour s'assurer que le traitement des données est conforme aux attentes de la CNIL.
- Les obligations de la personne responsable du traitement de données à caractère personnel :
  - certaines données à caractère personnel **ne peuvent pas être collectées** (origines, opinions politiques, orientation sexuelle...);
  - obligation de déclaration ou d'autorisation auprès de la CNIL ;
  - tout traitement de données à caractère personnel exige le consentement des personnes concernées ;
  - préserver la sécurité et la confidentialité des données :
    - exemple : si un commerçant stocke sur son site web les numéros de carte bancaire de ses clients, il devra mettre en place un dispositif de protection extrêmement robuste.

# Informatique et liberté: Le traitement automatisé des fichiers informatiques

- Avant d'envoyer des informations vous concernant sur le web, il est recommandé de vérifier les conditions indiquées dans les pages de mentions légales et de politique de confidentialité du site. Vous devez pouvoir y retrouver :
  - l'identité du responsable du site ;
  - l'objectif de la collecte d'informations ;
  - le caractère obligatoire ou facultatif des réponses fournies ;
  - les droits reconnus à la personne ;
  - les informations sur le traitement des données vous concernant.

# Informatique et liberté: Le traitement automatisé des fichiers informatiques

- Il est important de rester vigilant.
- Sur les réseaux sociaux de nombreuses données à caractère privé apparaissent et peuvent faire l'objet d'échanges entre certains réseaux sociaux et d'autres sites, notamment à partir des différentes options de partage, mais aussi de façon invisible pour vous.
- Une étude récente de chercheurs de l'Université de Cambridge au Royaume-Uni a démontré qu'avec la simple utilisation du bouton « J'aime » de Facebook, on peut dans 93 % des cas découvrir si la personne est un homme ou une femme et dans 95 % des cas, préciser l'origine ethnique de la personne. D'autres informations ont également pu être découvertes : choix politiques, orientations religieuses, sexuelles, addictions et dépendances potentielles.

# Informatique et liberté: Le traitement automatisé des fichiers informatiques

- La personne concernée par un traitement de données à caractère personnel bénéficie de droits :
  - d'information ;
  - d'accès ;
  - d'opposition ;
  - de rectification.
- En 2008 et 2009, la CNIL a reçu plusieurs plaintes émanant de clients d'une banque, dénonçant la persistance de leur inscription au fichier des impayés malgré la régularisation de leurs impayés auprès de l'établissement bancaire. La CNIL a mis en demeure la banque de mettre à jour les données de ses clients.



# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- RGPD
- La dématérialisation des services publics
- Modèles et stratégies économiques

# Les chartes et La nétiquette : définition

- La nétiquette est une notion beaucoup plus floue qu'une charte utilisateur, puisque ce terme recouvre des notions de **bonne conduite, de politesse, de courtoisie**, souvent plus difficiles à cerner. Sur Internet, la nétiquette est doublement importante. L'expression corporelle et le ton de la voix ne sont pas facilement exprimés par le texte (même en y ajoutant des émoticônes) et doivent donc être interprétés.

*« Ce que vous ne feriez pas lors d'une conversation réelle face à votre correspondant, ne prenez pas Internet comme bouclier pour le faire. » Wikipédia.*

# Les chartes et La nétiquette : : règles applicables au courriel

- Indiquer un **sujet** en rapport avec le contenu du message ;
- Commencer et terminer par une **formule de politesse** ;
- **Signer** le courriel ;
- **Ne pas citer la totalité** du message original, mais uniquement les parties spécifiques auxquelles vous répondez ;
- Mettre **les pièces jointes** dans un format lisible par le destinataire et dans une taille correcte ;
- Au cas où le courriel ressemble à un pourriel ou un canular informatique, **vérifier les informations** avant de les transmettre ;
- Si une information est à transmettre par courriel à plusieurs personnes qui ne se connaissent pas, placer leurs adresses en « **copie cachée** » (Bcc ou Cci) .

# Les chartes et La nétiquette : : règles applicables aux lieux d'échanges

- Les forums :
  - avant de poster un nouveau sujet, **vérifier** qu'il n'a pas déjà été traité précédemment ;
  - donner un **titre** pertinent au message ;
  - ne pas écrire en langage **SMS** ;
  - ne pas écrire en **MAJUSCULES** (signifie crier sur Internet).
- Les listes de diffusion :
  - avant de répondre à un message, **vérifier** si la réponse est envoyée à toute la liste ou seulement à l'expéditeur ;
  - éviter les comportements de **mail-bombing** ou **pourriel**.



# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- **RGPD**
- La dématérialisation des services publics
- Modèles et stratégies économiques

# RGPD: Données personnelles

- Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».
- Une personne peut être identifiée :
  - **directement** (exemple : nom, prénom)
  - **ou indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).
- L'identification d'une personne physique peut être réalisée :
  - **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
  - **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)
- **Exemple** : une base marketing contenant de nombreuses informations précises sur la localisation, l'âge, les goûts et les comportements d'achats de consommateurs, y-compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

# RGPD: Traitement de données personnelles

- Un « **traitement de données personnelles** » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).
- **Exemple** : tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.
- Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « [compagnieA@email.fr](mailto:compagnieA@email.fr) ») n'est pas un traitement de données personnelles.
- Un traitement de données doit avoir **un objectif**, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. A chaque traitement de données doit être assigné un **but**, qui doit bien évidemment être **légal et légitime au regard de votre activité professionnelle**.
- Un traitement de données personnelles n'est **pas nécessairement informatisé** : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

# RGPD: Définition

- Le sigle RGPD signifie « Règlement Général sur la Protection des Données » (en anglais « General Data Protection Regulation » ou GDPR). **Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne.**
- Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique, développement du commerce en ligne...).
- Ce nouveau règlement européen s'inscrit dans la continuité de la **Loi française Informatique et Libertés de 1978** et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.
- Il **harmonise les règles en Europe** en offrant un cadre juridique unique aux professionnels. Il permet de développer leurs activités numériques au sein de l'UE en se fondant sur la confiance des utilisateurs.

# RGPD: Qui est concerné?

- **Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné.**
- En effet, le RGPD s'applique à toute organisation, **publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :**
  - qu'elle **est établie sur le territoire de l'Union européenne,**
  - ou que son activité cible directement des **résidents européens.**
- **Par exemples,** une société établie en France, qui exporte l'ensemble de ses produits au Maroc pour ses clients moyen-orientaux doit respecter le RGPD. De même, une société établie en Chine, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.
- Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.
- Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

# RGPD: Les bonnes pratiques

## 1. Ne collectez que les données vraiment nécessaires

- Posez-vous les bonnes questions : Quel est mon objectif ?
- Quelles données sont indispensables pour atteindre cet objectif ?
- Ai-je le droit de collecter ces données ?
- Est-ce pertinent ?
- Les personnes concernées sont-elles d'accord ?

## 2. Soyez transparent

Une information claire et complète constitue le socle du contrat de confiance qui vous lie avec les personnes dont vous traitez les données.

## 3. Pensez aux droits des personnes

Vous devez répondre dans les meilleurs délais, aux demandes de consultation, de rectification ou de suppression des données.

## 4. Gardez la maîtrise de vos données

Le partage et la circulation des données personnelles doivent être encadrés et contractualisés, afin de leur assurer une protection à tout moment.

## 5. Identifiez les risques

Vous traitez énormément de données, ou bien des données sensibles ou avez des activités ayant des conséquences particulières pour les personnes, des mesures spécifiques peuvent s'appliquer.

## 6. Sécurisez vos données

Les mesures de sécurité, informatique mais aussi physique, doivent être adaptées en fonction de la sensibilité des données et des risques qui pèsent sur les personnes en cas d'incident.

# RGPD: Conservation des données clients

Dans le cadre de la conservation des données clients 3 règles sont à respecter :

- 1. Faites le tri !** Vendre un bien ou un service ne nécessite pas tout le temps le recueil de données personnelles. En revanche, pour établir une facture, livrer, offrir une garantie, instaurer une relation client sur la durée (exemple : abonnement), vous devez **informer votre client des données qui sont obligatoires pour rendre le service**. S'il est d'accord, votre client peut vous fournir plus d'informations pour que vous lui proposiez d'autres services optionnels
- 2. Au moment de la collecte, informez vos clients sur ce que vous faites de leurs données.** Insérez une rubrique « Protection des données », accessible et compréhensible par tous, dans vos conditions générales de vente. Prévoyez une mention d'information sur chaque formulaire de collecte. N'oubliez pas de leur fournir un moyen, simple et rapide, de vous contacter pour l'exercice de leurs droits d'accès, de rectification, d'opposition et d'effacement. Si vous souhaitez louer ou partager leurs coordonnées avec des partenaires commerciaux, n'oubliez pas de **demander à vos clients leurs préférences**. Si cela concerne leurs coordonnées électroniques, vous devrez recueillir leur **consentement**, dont vous devrez garder la preuve.
- 3. Ne gardez pas indéfiniment les données.** Prévoyez la **suppression** des informations en cas d'inactivité prolongée de vos clients (**3 ans à compter de la fin de la relation commerciale**). Vous devez toutefois conserver certaines données en raison **d'obligations légales** (notamment comptabilité, contentieux, etc.). Archivez-les dans une autre base de données dont l'accès est plus restreint.

# RGPD : Sur les Collaborateurs

- **Ne demandez à vos employés que les informations utiles pour accomplir leurs missions**, et évitez de traiter des données dites « sensibles » (activité syndicale, opinions politiques, religion, origine ethnique, santé). Si vous devez en traiter, des obligations particulières sont applicables.
- Vous disposez forcément **d'informations particulières** (et donc **à risque**) sur vos employés (coordonnées bancaires pour la paie, numéro de sécurité sociale pour les déclarations sociales, etc.). **Assurez-vous d'en garantir la confidentialité et la sécurité. Ainsi, seules les personnes habilitées doivent en prendre connaissance.** Les actions sur les données effectuées par les personnes habilitées doivent être enregistrées (savoir qui se connecte à quoi, quand et pour faire quoi).
- **Informez vos collaborateurs** à chaque fois que vous leur demandez des informations (exemple : mise à jour des données administratives, demande de formation, formulaire d'entretien d'évaluation, etc.).
- Enfin, souvenez-vous toujours que vos salariés peuvent vous demander une **copie de toutes les données les concernant que vous détenez** : copie d'un bulletin de paie, état d'un compte épargne-temps, mais aussi les enregistrements téléphoniques, relevés des badgeuses, ou encore des messages envoyés *via* le mail professionnel, y compris lorsqu'un employé n'est plus en poste ou est en litige avec vous.



# RGPD: Recrutement et surveillance

- **Lors d'un recrutement**, il faut demander la permission au candidat pour garder ses informations personnelles.
- **En cas de surveillance** des salariés, 2 règles simples son à retenir :
  1. **N'abusez pas de votre pouvoir !** la surveillance doit reposer sur un **intérêt légitime de l'entreprise** (exemple : limiter les risques d'abus d'une utilisation trop personnelle d'internet pendant le temps de travail); Les employés ne doivent pas être mis sous surveillance permanente (exemple : sécuriser un local professionnel n'impose pas de filmer en permanence un employé sur son poste de travail). N'utilisez pas un outil pour autre objectif caché (exemple : la géolocalisation des véhicules opérant une tournée chaque matin chez des clients pour optimiser votre organisation ne doit pas servir à contrôler la vitesse de circulation en temps réel).
  2. **Soyez transparent ! consultez les instances représentatives** du personnel et **informez les employés** de la mise en oeuvre d'un dispositif de surveillance, selon les modalités les plus appropriées en fonction de votre organisation (exemple : note de service, avenant au contrat de travail, mention d'information sur l'intranet, courrier joint au bulletin de paye, etc.).

# RGPD : La portabilité

- Le **droit à la portabilité**, créé par le RGPD, permet à toute personne de :
- recevoir **dans un format structuré, couramment utilisé et lisible par machine (ordinateur)** les données personnelles la concernant déjà fournies à un responsable de traitement ;
- faire transmettre **directement** ces données à un autre responsable de traitement **lorsque c'est techniquement possible**.
- <https://www.cnil.fr/fr/professionnels-comment-repondre-une-demande-de-droit-la-portabilite>

# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- RGPD
- La dématérialisation des services publics
- Modèles et stratégies économiques

# La dématérialisation des services publics: définition

- **Dématérialiser des documents** consiste à remplacer les **documents au format papier** de son organisation par des **fichiers numériques**, ou bien à les produire directement au **format numérique** via son **système d'information (dématérialisation native)**. Elle vise également à **stocker et conserver ses documents électroniques** sur des ordinateurs ou des serveurs informatiques.
- En plus de la **réduction des coûts de stockage** de fichiers papiers, la mise en place de la **dématérialisation des documents** permet de vrais **gains de productivité** grâce notamment à **l'automatisation du traitement des données** ou à une meilleure **gouvernance de l'information** (via la mise à disposition de tous les **documents sur support numérique** de l'entreprise pour les collaborateurs via un **point d'accès unique** sur internet ou via un intranet).
- Un **projet de dématérialisation** en entreprise est difficilement isolé car il vise à **revoir l'ensemble de la chaîne de gestion et de conservation des documents**. La dématérialisation peut donc concerner différents **processus de traitements** au sein des organisations et implique de les automatiser via la mise en place d'un **logiciel de Ged (gestion électronique des documents)**.
- Par ailleurs, la (bonne) **conservation des documents sur support numérique** (comment seront-ils conservés et pendant combien de temps) nécessite également la mise en place d'un **système d'archivage électronique (SAE)**. Celui-ci permet notamment de constituer un fond sécurisé des **documents probatoires et patrimoniaux** de l'entreprise et de garantir leur intégrité, puisqu'il empêche toute modification des données et des documents.

# La dématérialisation des services publics: Empreinte carbone

- A ce jour, **l'empreinte carbone des projets numériques** est insuffisamment prise en compte dans les projets de dématérialisation. Pourtant, le numérique représente 4 % des gaz à effet de serre (GES), et doublera d'ici 2025. La prise en compte des matériels informatiques, des usages ou encore du recyclage des déchets est donc urgent, dans une logique de bonne **gouvernance de l'information numérique**. De rares cabinets de conseil se sont d'ores et déjà emparés du sujet. **L'empreinte numérique de la dématérialisation** peut être divisée jusqu'à 3 fois.
- Cette prise en compte est un premier pas vers un nouveau modèle de développement d'entreprise, comme la **permaentreprise, le green IT...**

# Dématérialisation des services publics: Exemples

- La **dématérialisation** des services publics permet de faire en ligne la plupart des démarches.
  - Assurance maladie : [www.ameli.fr](http://www.ameli.fr)
  - [www.service-public.fr](http://www.service-public.fr) : papiers d'identité, permis de conduire, carte grise, etc.
  - Impots.gouv.fr pour déclarer ses impôts
- Elle se confronte cependant aux limites de la **fracture numérique** c'est-à-dire aux inégalités dans l'usage et l'accès aux technologies numériques.

# Sommaire

- Identification et e-reputation
- La loi informatique et liberté
- Les chartes et la nétiquette
- La dématérialisation des services publics
- **Modèles et stratégies économiques**

# Modèles et stratégies économiques: Exemples

Sur internet il existe différents modèles économiques, un peu différents des modèles industriels classiques, qui peuvent se compléter.

- **Le don** (ex : Wikipedia, Crowdfunding) ;
- **L'abonnement** (Ex : Netflix, Canal, OCS, beIN, Amazon, Disney+) ;
- **La publicité** est le modèle économique le plus connu elle est utilisée notamment par Google mais aussi par les réseaux sociaux comme Facebook ou Instagram (notamment du fait de la revente des données) ;
- **Le freemium** permet de donner à certains clients (contenu gratuit) pour mieux reprendre à d'autres (premium). Le service gratuit permet d'installer la marque et la diffuse. On note ainsi plusieurs acteurs (1) des hommes et des femmes, (2) des clients et des fournisseurs, (3) des clients et les annonceurs avec lesquelles une entreprise va pouvoir échanger en exploitant les externalités entre elles. Ce modèle a explosé avec le numérique. Ex : Spotify, Dropbox, Google, Airbnb, etc.



# Modèles et stratégies économiques: pratiques

- Internet a également contribué à faire émerger deux pratiques :
  - le **financement participatif**, ou **crowdfunding** qui consiste en un échange de fonds entre individus en dehors des circuits financiers institutionnels, afin de financer un projet, une association, via une plateforme en ligne.
    - Exemples de plateformes basées sur ce modèle économique : KissKissBankBank, ULULE, My Major Company, HelloAsso, Etc.
  - La **collecte d'argent en ligne** pour financer des événements publics ou privés :
    - Exemples de cagnottes en ligne : Leetchi, le Pot Commun, Lydia, etc.

# DSIUN – Service des usages numériques

- **Conception – Réalisation**

- Alexa Gallo – Catherine Loire – Mélanie Mauvoisin - Service des usages numériques - Université Paris 1 Panthéon-Sorbonne
- Mise à Jour 04/09/22 Valérie Monfort UFR27 - Université Paris 1 Panthéon-Sorbonne

- **Sources**

- Patricia Cavallo
- Martine Fontaine

---

Version du support : 2.0  
Septembre 2021



[Licence Creative Commons :](#)  
[Paternité - Pas d'Utilisation Commerciale](#)  
[Partage des Conditions Initiales à l'Identique](#)



UNIVERSITÉ PARIS 1  
**PANTHÉON SORBONNE**

---