Protection de la vie privée et des données personnelles

Guillaume Piolle
guillaume.piolle@centralesupelec.fr
http://guillaume.piolle.fr/

CentraleSupélec – mastère Cybersécurité

15 février 2017

L'enjeu de la vie privée dans les organisations

Une question éthique

Responsabilité de l'organisation (entreprise, administration, association...) vis-à-vis de ses salariés, de ses partenaires, de ses clients, de ses usagers, des personnes impactées par son activité.

Une question juridique

Obligation de **conformité** : loi informatique et libertés, directives et règlements européens, textes sectoriels divers...

Interaction avec le cadre juridique de la SSI et du support au judiciaire.

Une question technique

Problématique à prendre en compte, au même titre que la sécurité, lors de la conception des systèmes (propriétés techniques, architectures, méthodes et outils spécifiques).

Exemples de risques : brèches de vie privée

Formes principales

- Intrusion d'une personne dans vos affaires « privées » ;
- Révélation au public ou à un tiers d'une information « privée » que vous n'étiez pas prêt(e) à divulguer, et/ou qui est fausse ;
- Vol d'identité ;
- Profilage comportemental, prédiction comportementale, suivi...

Conséquences possibles

- Impact (plus ou moins grave) sur les relations sociales ;
- Risque de discrimination, d'influence, de limitation des choix ;
- Risque de poursuites ;
- Consommation de l'attention...

Et les personnes « publiques » ?

La vie privée : une notion liée à la culture

En France

Droit fondamental, et même « fondamental fondamental », condition nécessaire à l'exercice des autres droits fondamentaux.
Dans le bloc constitutionnel depuis 1971.
Rôle central de l'État comme garant de ce droit.

Aux États-Unis

Ne peut entrer en conflit avec la liberté d'expression, juridiquement supérieure (premier amendement).
Défiance envers l'État.
Rôle central du marché, de la libre entreprise.

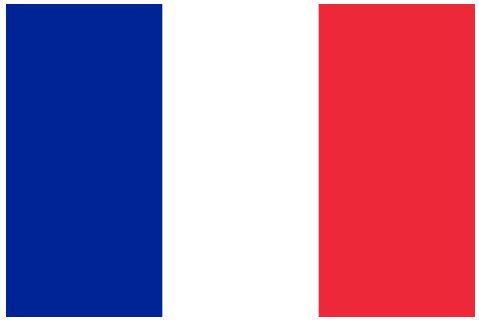
Historique

- Warren & Brandeis 1890 : *The Right to Privacy*. Premières réflexions suite aux progrès de la photographie ;
- Création progressive d'un droit à la vie privée dans la doctrine juridique, sous la forme d'un **droit de propriété incorporelle** lié aux **droits de la personne** ;
- 1970 : introduction du droit à la vie privée dans le Code civil français ;
- Fin des années 1970 : Scandale du fichier Safari, loi Informatique et Libertés ;
- Années 1990 et suivantes : trop denses pour être résumées ici !

Contexte international

- **ONU :**
  - 1948 - Déclaration universelle des droits de l'homme (art. 12) ;
  - 1966-1980 : Pactes à force contraignante (droits civils et politiques, droits économiques, sociaux et culturels).
- **Conseil de l'Europe :**
  - 1950 - Convention de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8) ;
  - 1981 - **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** (en particulier préambule, art. 5).
- **Union européenne :**
  - 1992-2007 - Traité de l'Union européenne (inclut la CSDHLF) ;
  - 2000-2010 - Charte des droits fondamentaux de l'Union européenne ;
  - 1995 : **Directive 95/46/CE**
  - 2002 : Directive 2002/58/CE
  - 2016 - **Règlement Général sur la Protection des Données** (RGPD / GDPR, en vigueur en 2018).

Contexte national en France



- **Code civil**, article 9 ;
- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés ;
- **Loi n° 2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (modifie 78-17) ;
- **Loi n° 2016-1321 du 7 octobre 2016** pour une République numérique (modifie 78-17).

`http://www.legifrance.gouv.fr/`

Droit à la vie privée *vs* Protection des données personnelles

Droit à la vie privée

Droit « correctif »
Notion de préjudice et de réparation
Il faut démontrer le préjudice

Protection des données personnelles

Droit « préventif »
Règles visant à éviter les violations de la vie privée
La violation des règles constitue un préjudice en soi, par principe

Loi Informatique et Libertés : Périmètre

Article 1

L'informatique doit être au service de chaque citoyen.

Son développement doit s'opérer dans le cadre de la **coopération internationale**.

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**.

Loi Informatique et Libertés : Périmètre

Article 2 (extrait)

La présente loi s'applique aux **traitements automatisés de données à caractère personnel**, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles [...].

Infractions à la loi Informatique et Libertés

- Sanction administrative : jusqu'à 3 M€ (depuis 2016) puis 20 M€ (à partir de 2018) ;
- Sanction pénale : 5 ans de prison et 300 000 € d'amende ($\times$ 5 pour les personnes morales) (art. 226-16 à 226-24 du Code pénal) ;

Loi Informatique et Libertés : Périmètre

Donnée à caractère personnel (donnée personnelle)

Suite de l'article 2 :

Constitue une donnée à caractère personnel **toute information relative à une personne physique identifiée ou qui peut être identifiée**, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer **l'ensemble des moyens** en vue de permettre son identification dont dispose ou auxquels peut avoir accès **le responsable du traitement ou toute autre personne**.

Avant 2004 (cf directive 95/46), on parle d'*informations nominatives* ou *indirectement nominatives*.

Au niveau européen : « moyens susceptibles d'être raisonnablement mis en œuvre ».

I&L : Acteurs

Les acteurs décrits par la loi

- Le responsable de traitement ;
- La personne concernée (sujet des données) ;
- Les destinataires ;
- Les sous-traitants ;
- La CNIL ;
- Le CIL (futur DPD/DPO).

I&L : Principe de légalité

Données sensibles (art. 8)

Il est interdit de procéder à des traitements portant sur des données sensibles :

- Origines raciales ou ethniques ;
- Opinions politiques, philosophiques, religieuses ;
- Appartenance syndicale ;
- Santé et vie sexuelle.

Exceptions : consentement exprès, sauvegarde de la vie humaine, gestion des listes de membres, données déjà rendues publiques par la personne concernée, services de santé, statistiques officielles, recherche médicale, « intérêt public » (strictement encadré).

I&L : Principe de finalité

Art. 6, 2°

On collecte des données personnelles en vue d'une **finalité** déterminée (et pas « au cas où »).

On ne peut pas utiliser les données *de manière incompatible* avec la finalité initialement prévue.

I&L : Principe de légitimité

Art. 6, 2°

La finalité déclarée doit être **légitime**.

Voir le rôle du responsable de traitement vis-à-vis de la personne concernée : est-ce une finalité légitime pour une société de transports en commun de mettre en place des traitements de données visant à la gestion d'une régie publicitaire ?

cf. notion d'**intérêt légitime** comme fondement au traitement.

I&L : Principe de proportionnalité

Art. 6, 3°

La collecte doit être **proportionnée** (nature et quantité des données) à la finalité.

Données « adéquates, pertinentes et non excessives », + objectives et licites.

Adéquation de la durée de conservation (5°)

Pour des contre-exemples, voir 95 % des formulaires d'inscription sur Internet...

I&L : Formalités préalables

Régime de déclaration

Cas par défaut (pas de données sensibles). Dispense de déclaration si présence d'un CIL dans l'organisation, ou pour certains traitements jugés sans risque par la CNIL.

Régime d'autorisation (ou avis)

Traitements portant sur des données sensibles, génétiques, biométriques, relatives aux infractions ou condamnations, ou susceptibles de priver d'un droit, ou utilisant le numéro INSEE...

La mise en place d'un IPS ou d'un IDS relève d'un régime d'autorisation ! (voire est illicite au regard de l'article 9 de la loi... pouf pouf).

I&L : Droits et obligations

Droits des personnes concernées

- Obligation d'information sur le traitement, la collecte, la conservation, la transmission des données (art. 32) ;
- Droit d'accès (art. 39) et de rectification (art. 40) ;
- Droit d'opposition *pour des motifs légitimes* (art. 38) ;
- Droit de suppression *en cas de non-conformité* ou si la personne est mineure (art. 40).

I&L : Mentions obligatoires

À faire figurer lors de la collecte :

- Droits des personnes ;
- Identité du responsable de traitement ;
- Finalité du traitement ;
- Durée de conservation (depuis 2016) ;
- Destinataires des données ;
- Existence de flux transfrontaliers ;
- (Pour un questionnaire) caractère obligatoire ou facultatif des réponses ;
- (Pour un questionnaire) conséquences d'un défaut de réponse.

I&L : Obligations du responsable de traitement

Garantie des droits et des principes

Le responsable de traitement doit garantir les principes de légalité, de finalité, de légitimité et de proportionnalité, ainsi que les droits des personnes concernées (notamment via les « mentions obligatoires »).

Obligation de sécurité

Le resp. de traitement ne devient pas nécessairement propriétaire des données (notion assez floue d'ailleurs), mais doit assurer « la sécurité des traitements et des données » et empêcher qu'elles soient « déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Destruction des données

Le responsable de traitement ne peut conserver (telles quelles) les données à l'issue de la période de conservation déclarée. La destruction est généralement recommandée, mais la loi permet en théorie « l'anonymisation » (attention, casse-gueule...).

Commission Nationale de l'Informatique et des Libertés

Première autorité administrative indépendante en France (même statut que la Hadopi, par exemple).

Créée par la loi de 78, compétences modifiées par les lois de 2004 et 2016.

Membre français du G29.

Mission d'**information** et de **contrôle**.

`http://www.cnil.fr/`, nombreuses ressources en ligne (mais de moins en moins accessibles depuis la refonte de leur site web. . .)

Encadrement des formalités préalables

La CNIL. . .

- Est destinataire des déclarations normales et simplifiées ;
- Délivre les autorisations pour les traitements portant sur des données sensibles ;
- Émet des avis sur les traitements mis en œuvre par arrêté ministériel, par décret en Conseil d'État ou par certains organismes en situation de service public ;
- Répond aux demandes d'accès indirect ;
- Peut délivrer des « labels ».

La CNIL doit être consultée sur tout projet de loi ou de décret concernant son périmètre juridique et peut faire des propositions législatives ou réglementaires.

Mission de contrôle-sanction

La CNIL. . .

- Organise des contrôles spontanés auprès des responsables de traitements ;
- Reçoit les « réclamations, pétitions et plaintes » et éventuellement y donne suite ;
- En cas de saisine ou de constatation d'une infraction, la CNIL peut :
  - Classer sans suite ;
  - Organiser une médiation ;
  - Procéder à un contrôle ;
  - Émettre un avertissement, une mise en demeure, une injonction de cesser le traitement, un retrait d'autorisation ;
  - Infliger elle-même une sanction (~~jusqu'à 150 000 €, puis 300 000 € plafonnés à 5 % du CA en cas de récidive~~ porté à 3 000 000 € en 2016).

La CNIL doit informer le procureur de la République des infractions dont elle a connaissance.

Statistiques sur l'activité de contrôle-sanction

Exemple : le rapport d'activité 2009

- Évolution constante du nombre de contrôles (de 96 en 2005 à 270 en 2009) ;
- Principaux manquements constatés en contrôle :
  - Collecte déloyale (27 %) ;
  - Pertinence et mise à jour des données (23 %) ;
  - Information, droit d'accès ou d'opposition (19 %) ;
  - Communication à des tiers non autorisés (6 %) ;
  - Sécurité et confidentialité des données (6 %) ;
  - Défaut de consentement préalable (5 %).

Critique de la CNIL

Rendue « inoffensive » pour l'État

Depuis la loi de 2004, la CNIL n'a plus de pouvoir de contrôle sur l'État. Elle ne fait qu'émettre un **avis**, qui n'est pas nécessairement suivi (il faut alors un décret en Conseil d'État. . . mais l'avis du CE n'est pas nécessairement suivi non plus par le gouvernement).

Une autorité de contrôle trop complaisante ?

Sanctions souvent jugées beaucoup trop faibles en regard des infractions (beaucoup d'avertissements sans réelles conséquences, amendes très rares et généralement faibles).
Cet état de fait participe sans doute du peu d'effectivité de la protection des données personnelles.

Correspondant Informatique et Libertés

Interlocuteur privilégié de la CNIL, nommé dans une organisation (publique ou privée).
Sa présence dispense l'organisation des déclarations (un registre est tenu en interne), pas des demandes d'autorisation.
Le CIL :

- Répertorie les traitements et s'assure qu'ils sont conformes à la loi ;
- Assure l'accès au registre ;
- Dispose d'un contact privilégié à la CNIL, ainsi que d'un réseau ;
- Établit un bilan annuel d'activité, tenu à disposition de la CNIL ;
- A une mission d'assurance qualité, de conseil, de vigilance.

Profil-type du CIL

Informaticien, juriste d'entreprise, auditeur, avocat...

Rattachement à l'organigramme lui assurant l'indépendance (idéal : **secrétariat général, DG, présidence**, mais on trouve aussi RH, RSSI, département juridique...

Le CIL deviendra, avec le règlement, un « délégué à la protection des données » (DPD, ou DPO pour *Data Protection Officer*). Il héritera alors d'une mission de contrôle (associée à une responsabilité individuelle ? pas clair).

Les flux transfrontaliers

Cas 1 : Union européenne

Au sein de l'Union européenne, ce ne sont pas des flux transfrontaliers – mêmes disposition que si les données restaient en France.

Cas 2 : pays proposant « un niveau de protection adéquat »

11 pays : Andorre, Argentine, Canada, Man, Féroé, Israël, Jersey, Guernesey, NZ, Suisse, Uruguay.
Simple déclaration en sus des formalités standard.

Les cas particuliers

- Entreprises US du ~~*Safe Harbor*~~ *Privacy Shield* : *cf.* cas 2 ;
- Exceptions légales (art. 69, limitation aux cas ponctuels et exceptionnels) : idem que pour le cas 2 ;
- Clauses contractuelles types (fournies par l'UE), *Binding Corporate Rules* au sein d'un même groupe : décision d'autorisation de la CNIL.

Les moyens de recours

Saisine de la CNIL

Par tout moyen (formulaire web, lettre simple). Doit agir dans les deux mois.
Actions possibles : classer sans suite, organiser une médiation, contrôle, avertissement, mise en demeure, injonction de cesser le traitement, retrait d'autorisation, sanction financière.

Action en justice (saisine du procureur, citation, assignation. . .)

Possible, mais il peut être mal vu de court-circuiter la CNIL. Avocat obligatoire au civil, fortement recommandé au pénal.

Depuis 2016, possibilité d'un recours collectif, limité à la cessation du manquement (pas de réparation du préjudice).

Les finalités de recherche

Plusieurs domaines d'activités bénéficient de cadres juridiques d'exception pour la protection des données personnelles : défense / sécurité nationale, justice / police judiciaire, santé publique, recherche médicale, journalisme, archives, statistiques nationales...

Quelques exceptions applicable à la recherche scientifique, historique [ou statistique] (hors recherche médicale)

- Possibilité de réutiliser des données issues d'un autre traitement (avec une autre finalité) : les finalités de recherche sont considérées comme « compatibles » par défaut ;
- Possibilité de conserver indéfiniment des données pour ces (seules) finalités, sans nécessairement en informer les personnes concernées ;
- (Depuis 2016) Cadre spécifique pour l'utilisation du NIR ;
- Limitation du droit d'accès/rectification/suppression dans certains cas ?

Le RGPD / GDPR : qu'est-ce qui change en 2018 ?

Principes généraux

- Notion de **guichet unique** pour les entreprises ;
- Diminution / suppression des formalités préalables pour les traitements jugés sans risques, mais davantage de mesures pour les traitements « risqués ».

Problème : dans la majorité des cas, c'est le responsable de traitement qui évalue seul le risque...

Consentement (art. 7), révocation et droit à l'oubli (art. 17)

- Renforcement de l'importance du consentement (explicite, libre, informé, distinct et révocable pour chaque traitement) ;
- Renforcement d'un droit à l'effacement / droit à l'oubli explicitement mentionné.

Impact finalement limité, la proportion des traitements s'appuyant sur un consentement étant assez faible.

Le RGPD / GDPR : qu'est-ce qui change en 2018 ?

Mise à jour des données sensibles (art. 9)

Ajout des **données génétiques** et de la **biométrie** à fins d'identification

Accountability

- Obligations de **journalisation** et **d'auditabilité** plus lourdes pour les responsables de traitement (cf. charge de la preuve, notamment pour le consentement) ;
- Obligation de **notification** à l'autorité de contrôle de toute « violation de données à caractère personnel » constatée, sous 72h *si possible* (sauf si non « susceptible d'engendrer un risque »).
  Notification aux personnes concernées seulement en cas de « risque élevé », et seuelement « dans les meilleurs délais ».

Le RGPD / GDPR : qu'est-ce qui change en 2018 ?

Études d'impact (art. 35)

Obligation d'effectuer un *privacy impact assessment* (PIA) est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ». Notamment :

- Profilage (ou évaluation systématique et approfondie d'aspects personnels) conduisant à une décision produisant des effets juridiques ou affectant significativement une personne ;
- Traitement à grande échelle de données sensibles ou relatives aux infractions ;
- Surveillance systématique à grande échelle d'une zone accessible au public.

Identification d'un risque élevé en l'absence de contremesures → « consultation » de l'autorité (CNIL).

Le RGPD / GDPR : qu'est-ce qui change en 2018 ?

Le DPD / DPO (art. 37-39)

Le « délégué à la protection des données » (CIL) devient obligatoire dans :

- Les organisations publiques ;
- Celles dont les activités de base exigent « un suivi régulier et systématique à grande échelle des personnes » ;
- Celles dont les activités de base consistent à traiter à grande échelle des données sensibles ou relatives à des condamnations ou infractions.

Son indépendance doit être garantie.
Évolution par rapport au CIL : ajout d'une **mission de contrôle**, possiblement assortie de l'engagement de sa responsabilité individuelle.

Le RGPD / GDPR : qu'est-ce qui change en 2018 ?

Sanctions (art. 83-84)

- Sanctions administratives graduées (en sus des sanctions pénales nationales et des autres actions des autorités nationales), allant jusqu'à 20 M€ ou 4% du CA mondial (montant le plus élevé).

Autres dispositions

- Droit à la portabilité des données (art. 20) ;
- Droit extrêmement limité à ne pas faire l'objet d'une décision automatisée ou d'un profilage (art. 22) ;
- Protection spécifique des mineurs (clarté de l'information, âge du consentement, révocation après la majorité) ;
- *Data protection by design* et *data protection by default* ;
- Possibilité de certification des traitements.

Données personnelles et vie privée au travail

Principe général

Dans le cas général, le salarié a le droit d'utiliser ponctuellement les moyens mis à sa disposition par son employeur pour des fins personnelles. Il ne doit bien sûr pas en abuser...

L'accès de l'employeur aux e-mails

Arrêt « Nikon » (2001) de la chambre sociale de la Cour de cassation
Si un e-mail est marqué comme personnel, ou classé dans un dossier confidentiel, l'employeur ne peut en prendre connaissance (secret des correspondances).
Dans les autres cas, il y a présomption de caractère professionnel.

Données personnelles et vie privée au travail

L'accès de l'employeur aux fichiers

Arrêt « The Phone House » (2007) de la chambre sociale de la Cour de cassation : extension du principe aux fichiers (y compris la présomption de caractère professionnel).

Arrêt de 2005 : « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

Chambre sociale, 2011 : « Si l'employeur peut toujours consulter les fichiers qui n'ont pas été identifiés comme personnels par le salarié, il ne peut les utiliser pour le sanctionner s'ils s'avèrent relever de sa vie privée. »

Données personnelles et vie privée au travail

Arrêt de 2009 : l'administrateur « est tenu d'une **obligation de confidentialité** » (même vis-à-vis de l'employeur) et peut accéder aux données des courriers électroniques échangés par les salariés uniquement « dans le cadre de sa mission de sécurité du réseau informatique ».

Et pour la consultation de sites web ?

À ma connaissance, pas d'arrêt de la Cour de cassation dans ce sens...

L'employeur a, a priori, le droit de connaître les sites web consultés par les salariés (et de capturer le contenu des interactions ?).

Données personnelles et vie privée au travail

Géolocalisation des salariés

Particulièrement pertinent pour les sociétés de transport : maintien de statistiques sur les trajets, contrôle des itinéraires...

La CNIL considère que le salarié doit pouvoir désactiver le dispositif à l'issue de son temps de travail.

Attention à la finalité déclarée du traitement : si c'est les stats et l'optimisation, impossible de s'en servir à titre disciplinaire contre le salarié.

Attention également si le salarié dispose de la liberté d'organisation de son temps de travail.

Données personnelles et vie privée au travail

~~Vidéosurveillance~~ Vidéoprotection au travail

Finalités autorisées : sécurité des biens et des personnes (dissuasion, identification des responsables)

- **On peut filmer :** entrées et sorties des bâtiments, issues de secours, voies de circulations, zones de stockage de marchandises...
- **On ne peut pas filmer :** employés sur leur poste de travail, zones de pause ou de repos, toilettes, locaux syndicaux et de RP (y compris leur accès).

→ Accès limité (au personnel de sécurité, pas aux RH ou à la direction !)
→ Conservation limitée à **un mois**

Formalités auprès de la CNIL, de la préfecture (suivant les cas), des instances représentatives du personnel.
Chaque employé doit être informé **individuellement**, en sus de l'affichage obligatoire.

La vie privée selon l'ISO

Common Criteria for Information Technology Security Evaluation

Norme ISO/IEC 15408, successeur de l'*Orange Book* du DoD.
Section 7 : protection de la vie privée.

Exigences techniques pour assurer la vie privée

- **Anonymat** (*anonymity*) : incapacité des observateurs à déterminer l'identité d'un utilisateur ;
- **Pseudonymat** (*pseudonymity*) : idem, mais en imposant à l'utilisateur de répondre de ses actions ;
- **Non-chaînabilité** (*unlinkability*) : incapacité des observateurs à déterminer si deux actions ont été réalisées par le même utilisateur ;
- **Non-observabilité** (*unobservability*) : incapacité des observateurs à déterminer si une action est en cours.

Souveraineté des données

Faire en sorte que **l'utilisateur conserve le contrôle** sur les données personnelles le concernant :

- Stocker en priorité données et/ou clés sur ses terminaux personnels ;
- Contrôler étroitement usage et diffusion, en imposant des obligations (obligations de sécurité, notifications, suppression...).

Souveraineté au sens juridique : attention toute particulière à porter aux données externalisées, en particulier lorsque le prestataire est de droit US, et ce **même si les données sont stockées dans l'union européenne** : le *Stored Communication Act*, le *PATRIOT ACT* et *FISAA* permettent à l'administration US d'accéder aux données, silencieusement, et pour des motifs pouvant parfois relever de simples intérêts économiques (cf. analyses et recommandations SGDSN, délégation interministérielle à l'intelligence économique, Parlement européen).

Minimisation des données

Minimisation des données

cf. principe de proportionnalité

- Ne collecter que les données absolument nécessaires à la finalité ;
- Ne les transmettre/conserver que si c'est absolument nécessaire ;
- Détruire dès que possible les données non absolument nécessaires ;

Le tout dans les limites des obligations d'auditabilité des systèmes.

Le problème, c'est que dans certains cas d'usage il n'est pas facile, voire impossible, de savoir à l'avance quelles données vont être utiles/nécessaires. . . Ce n'est pas quelque chose que la CNIL ou un CIL aime forcément entendre !

Le *Privacy by Design*

Principe

La protection de la vie privée, comme la sécurité, ne peut être efficace que si elle est pensée dès la conception du système. Les ajouts postérieurs ne peuvent pas espérer colmater des brèches de conception.

Le principe, de plus en plus mentionné dans les textes, doit concerner à la fois les intervenants techniques et non techniques, conjointement.

Exemples de mise en œuvre :

- Travail de spécification incluant experts techniques, juristes et décideurs ;
- Application de méthodes formelles de conception ;
- *Privacy impact assessments* ;
- Systèmes contraints par les politiques ;
- ...

Le *Privacy by Design*

Les sept principes du PbD

- Proactif plutôt que réactif, préventif plutôt que correctif ;
- Considérer la protection de la vie privée comme le réglage par défaut (*Privacy by default*) ;
- Intégrer la protection de la vie privée dans la conception du système ;
- Assurer des fonctionnalités complètes : viser une somme positive, pas une somme nulle ;
- Assurer la sécurité de bout en bout, avec une protection tout au long du cycle de vie ;
- Visibilité et transparence – viser l'ouverture ;
- Montrer du respect pour la vie privée des utilisateurs – centrer les systèmes sur les utilisateurs.

Sources

- CNIL, *Ce que change la loi pour une République numérique pour la protection des données personnelles* (`https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles`), 17 novembre 2016.