ANITEC

ALLIANCE NATIONALE
DES INTÉGRATEURS DE TECHNOLOGIES
CONNECTÉES, SÉCURISÉES ET PILOTÉES

Dossier RGPD:

TOUT SAVOIR SUR:
Le règlement général sur la protection des données

Alliance Nationale des Intégrateurs de Technologies connectées, sécurisées et pilotées.
5, rue de l'Amiral Hamelin / 75116 Paris / +33 1 44 05 84 40 / contact@anitec.fr
anitec.fr
SIRET 840 853 956 000 18 / APE : 9411Z / Syndicat : 201 800 16 / 21 444.

ANITEC
ALLIANCE NATIONALE
DES INTÉGRATEURS DE TECHNOLOGIES
CONNECTÉES, SÉCURISÉES ET PILOTÉES

SOMMAIRE

Alliance Nationale des Intégrateurs de Technologies connectées, sécurisées et pilotées.

5, rue de l'Amiral Hamelin / 75116 Paris / +33 1 44 05 84 40 / contact@anitec.fr

anitec.fr

SIRET 840 853 956 000 18 / APE : 9411Z / Syndicat : 201 800 16 / 21 444.

SÛRETÉ / VIDÉOSURVEILLANCE

RGPD : Les traitements dispensés d'une analyse d'impact

Délibération n° 2019-118 du 12 septembre 2019 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise (JO du 22 octobre 2019, texte n° 90).

La Commission Nationale Informatique et Libertés [CNIL] a fait paraitre le 22 octobre 2019, une liste des opérations de traitement pour lesquelles une analyse d'impact (AIPD) relative à la protection des données n'est pas obligatoire.

Pour rappel et depuis le 25 mai 2018, le RGPD impose d'effectuer une analyse d'impact (AIPD) avant tout traitement à risque élevé pour les droits et libertés des personnes concernées (RGPD, art. 35).

Cette procédure vise à «responsabiliser» les responsables de traitement et les sous-traitants qui manipulent des données à caractère personnel et permet de limiter l'obligation de déclaration préalable à l'autorité de contrôle aux seuls traitements susceptibles d'engendrer ces risques élevés.

L'analyse d'impact est également obligatoire dans 3 cas (RGPD, art. 35, § 3) :

- L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement informatisé (y compris le profilage) et sur la base de laquelle sont prises des décisions produisant des effets juridiques [ressources humaines, marketing];
- Le traitement à grande échelle de catégories particulières de données (RGPD, art. 9, § 1), ou de données à caractère personnel relatives à des condamnations pénales et infractions ;
- La surveillance systématique à grande échelle d'une zone accessible au public [vidéosurveillance, vidéoprotection].

La liste adoptée par la CNIL se présente sous la forme du tableau suivant :

La mise en œuvre d'un traitement figurant sur la présente liste ne dispense pas le responsable de traitement du respect de ses autres obligations prévues par le RGPD. Les traitements, même exonérés d'analyse d'impact, doivent faire l'objet d'une évaluation de leur conformité au RGPD tant sur le plan juridique qu'en matière de sécurité.

En cas de doute quant à la nécessité d'effectuer une AIPD il est recommandé d'en effectuer une.

D'autre part, la CNIL indique à ce titre dans sa délibération que, notamment, le fait qu'une activité de traitement relève de cette «liste de dispenses» ne signifie pas qu'un responsable de traitement est exempté des obligations en matière de sécurité du traitement (nécessitant, par exemple, la pseudonymisation ou le chiffrement des données à caractère personnel (RGPD art. 32).

Types d'opérations de traitement	Exemples
Traitements, mis en œuvre uniquement à des fins de ressources humaines (gestion du personnel des organismes qui emploient moins de 250 personnes, à l'exception du recours au profilage).	• la gestion de la paye, l'émission des bulletins de salaire ; • la gestion des formations ; • la gestion du restaurant d'entreprise, la délivrance des chèques repas ; • le remboursement des frais professionnels ; • le contrôle du temps de travail ; • le suivi des entretiens annuels d'évaluation ; • la tenue des registres obligatoires ; • l'utilisation d'outils de communication (messagerie électronique, téléphonie, vidéoconférences, outils collaboratifs en ligne) sans recours au profilage ni à la biométrie ; • le contrôle du temps de travail (sans dispositif biométrique, sans données sensibles ni à caractère hautement personnel).
Traitements de gestion de la relation fournisseurs.	• d'effectuer les opérations administratives liées : aux contrats ; aux commandes ; aux réceptions ; aux factures ; aux règlements ; à la comptabilité pour ce qui a trait à la gestion des comptes fournisseurs ; • d'établir les titres de paiement (traites, chèques, billets à ordre...) ; • d'établir des statistiques financières et de chiffre d'affaires par fournisseur ; • de fournir des sélections de fournisseurs pour les besoins de l'entreprise ou de l'organisme ; • d'entretenir une documentation sur les fournisseurs.
Traitements destinés à la gestion des activités des comités d'entreprise et d'établissement.	• de gérer les programmes socio-culturels de l'entreprise, communication interne ; • la formation des élus ; • l'exercice du droit d'alerte de l'article L2312-59 du Code du travail ; • la gestion des agendas et réunions ; -la gestion de leurs membres.
Traitements mis en œuvre par une association, une fondation ou toute autre institution sans but lucratif pour la gestion de ses membres et de ses donateurs dans le cadre de ses activités habituelles dès lors que les données ne sont pas sensibles.	• la gestion administrative des membres et donateurs, en particulier la gestion des cotisations ; • d'établir pour répondre à des besoins de gestion, des états statistiques ou des listes de membres ou de contacts, notamment en vue d'adresser bulletins, convocations, journaux. (les critères retenus devant être objectifs et de fonder uniquement sur des caractéristiques qui correspondent à l'objet statutaire de l'organisme) ; • d'établir des annuaires de membres, y compris lorsque ces annuaires sont mis à la disposition du public ou sur le réseau internet ; • d'effectuer par tout moyen de communications des opérations relatives à des actions de prospection auprès des membres, donateurs et prospects.

Types d'opérations de traitement	Exemples
Traitements mis en œuvre aux seules fins de gestion des contrôles d'accès physiques et des horaires pour le calcul du temps de travail, en dehors de tout dispositif biométrique. A l'exclusion des traitements des données qui révèlent des données sensibles ou à caractère hautement personnel.	• la mise en place d'un dispositif par badge sans biométrie pour entrer dans les locaux d'un organisme à des fins de sécurité ; • la mise en place d'un dispositif de contrôle du temps de travail effectué par les salariés, à l'exclusion de toute autre finalité.
Traitements relatifs aux éthylotests, strictement encadrés par un texte et mis en œuvre dans le cadre d'activités de transport aux seules fins d'empêcher les conducteurs de conduire un véhicule sous l'influence de l'alcool ou de stupéfiants.	• Les traitements ayant pour finalité la mise en place d'éthylotests «anti-démarrage» dans des camions de transport.

Veille Juridique n°4

Mise en conformité juridique des systèmes de vidéoprotection [Impact du Règlement Général sur la Protection des Données]

Attention ! Dans les documents officiels, les entreprises d'installation, d'intégration et de maintenance sont définies comme « sous-traitant ». Nous reprenons dans cette note la terminologie juridique de désignation pour les entreprises adhérentes de l'ANITEC.

Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) est entré en application. La plupart des formalités auprès de la CNIL ont disparu. C'est le cas des déclarations de vidéosurveillance dans les zones privées (par exemple les lieux de travail non-ouverts au public).

Toutefois, conformément au RGPD, les DPO [Délégués à la Protection des Données] donneurs d'ordres travaillant avec les adhérents ANITEC devront mettre en œuvre des modalités précises d'information des personnes filmées dans ces zones privées, nous recommandons aux spécialistes intégrateurs de solutions en sécurité électronique de diffuser à leurs clients actuels ou futurs, cette information. Pour cela, veuillez suivre les recommandations de la CNIL en cliquant sur le lien ci-après :

https://www.cnil.fr/fr/RGPD-exemple-information-salaries-videosurveillance-au-travail

De plus, si vous avez désigné un DPO au sein de votre entreprise intégratrice, ce dernier doit être associé à la mise en œuvre des caméras. Si le dispositif doit faire l'objet d'une analyse d'impact (EIVP), le DPO doit y être associé.

Ce point concerne l'intégrateur comme le DPO donneur d'ordre. C'est au DPO donneur d'ordre de mettre en œuvre l'analyse d'impact.

Toutefois, l'intégrateur doit pouvoir accompagner le DPO donneur d'ordre par son « devoir de conseil » en qualité de sous-traitant, et s'assurer avec lui, que le résultat de l'identification de TOUTES les menaces et vulnérabilités portant sur les données personnelles SOIT neutralisé au travers du plan de traitement, qui doit regrouper l'ensemble des préconisations.

ATTENTION ! *Si les formalités de déclaration CNIL, d'un système de vidéoprotection disparaissent. Le responsable du traitement donneur d'ordre devra s'assurer que son risque soit suffisamment identifié et atténué au travers de l'EIVP. Le refus de mise en œuvre d'une étude d'impact, ou une étude d'impact insuffisamment déployée, obligerait le responsable de traitement donneur d'ordre à une consultation auprès de*

Nous contacter : 5 rue de l'Amiral Hamelin - 75116 PARIS - Tél : 01 44 05 84 40
Mail : k.clement@anitec.fr - WWW.svdi.fr

la CNIL pour faire valider son projet, conformément au 2 de l'article 36. Dans ce cas, c'est l'ensemble du projet qui pourrait être mis en péril du fait des délais retenus :

- Lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant,
- Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation,

Cas des donneurs d'ordres sans DPO : [Petits commerces, petits établissements, marché domestique pour les domoticiens professionnels], c'est à l'intégrateur de porter l'EIVP et par le biais de la mise en œuvre de son « devoir de conseil » de devenir un « tiers de confiance » pour son client. Dans ce cas de figure, l'intégrateur s'assurera que son étude d'impact SOIT optimale pour éviter l'écueil de l'article 36 du RGPD. **Pour cela, veuillez suivre les recommandations de la CNIL en cliquant sur le lien ci-après :**

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Vous devrez inscrire ce dispositif de vidéosurveillance dans le registre des traitements de données que vous devrez tenir. Pour l'adhérent ANITEC, vous devrez disposer d'un « Registre de traitement type responsable du traitement » pour ce qui concerne la gestion administrative de votre entreprise mais également d'un « Registre de traitement type sous-traitant » pour référencer et stocker le résultat de vos analyses d'impacts. **Pour cela, veuillez suivre les recommandations de la CNIL en cliquant sur le lien ci-après :**

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

ATTENTION ! *Les systèmes installés sur voie publique ne dépendent que du Code de Sécurité Intérieure et de l'article 9 du Code Civil », il n'y a pas d'interaction RGPD.*

Quelles sont les sanctions en cas de non-déclaration d'un système de vidéosurveillance ?

Pour le RGPD, les moyens dissuasifs mis à la disposition de l'autorité de contrôle se trouvent à l'article 58 §2 du RGPD. L'intervention de l'autorité de contrôle est progressive. Les sanctions sont donc graduées en fonction de la violation du RGPD,

- Etape 1 : Avertissement ou une mise en demeure de l'entreprise fautive avec rappel du devoir de mise en conformité des traitements de données sensibles au RGPD,
- Etape 2 : Injonction de cesser la violation,
- Etape 3 : Limitation ou suspension temporaire des traitements de données,

- Etape 4 : Sanctions administratives en cas de non-respect aux règles du RGPD après injonction vaine de l'autorité de contrôle.

L'article 83 du RGPD liste les conditions, pour imposer une sanction administrative à un organisme ayant violé une des règlementations du RGPD. Ces facteurs doivent être pris en compte pour fixer un montant d'amende proportionnel, dissuasif et effectif par rapport à la violation du règlement européen.

Exemple de violation: L'absence de tenue d'un registre des traitements ou l'absence d'analyse d'impact préalable aux traitements des données personnelles.

Dans le cas d'infractions plus graves liées à la mauvaise application ou au non-respect du RGPD, une amende qui correspond à 4 % du chiffre d'affaires mondial s'agissant des entreprises ou 20 millions d'euros d'amende.

Les sanctions pénales pouvant être retenues dans le cadre du RGPD

« Atteintes aux droits de la personne dans le cas des fichiers ou des traitements informatiques » (articles 226-16 à 226-24) du Code pénal. Il existe donc par exemple une sanction pénale en cas de détournement de la finalité des données personnelles lors d'un traitement de données (Article 226-21 du Code pénal). Les sanctions pénales peuvent aller jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende (Article 226-16 du Code pénal)

Quelles sont les conditions à respecter avant de mettre en place des dispositifs de vidéosurveillance ?

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_commerces.pdf

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf

https://www.cnil.fr/sites/default/files/atoms/files/videosurveillance_immeubles_habitation.pdf

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_etablissements_scolaires.pdf

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_chez_soi.pdf

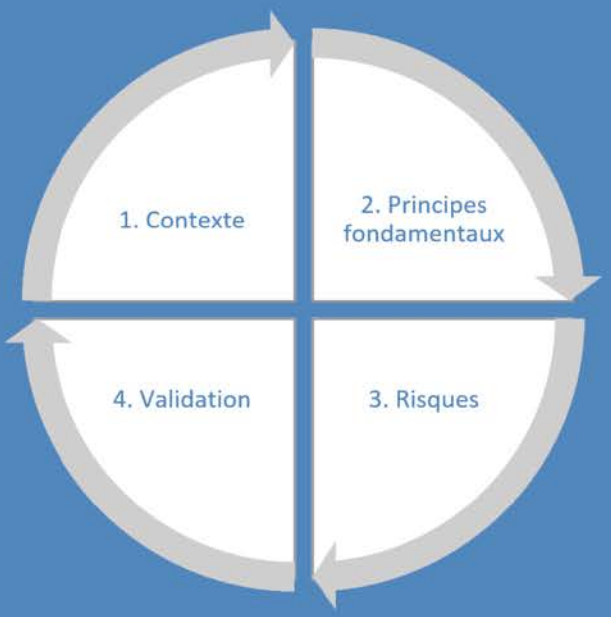
https://www.cnil.fr/sites/default/files/atoms/files/videosurveillance_voie_publique.pdf

Nous contacter : 5 rue de l'Amiral Hamelin - 75116 PARIS - Tél : 01 44 05 84 40
Mail : k.clement@anitec.fr - WWW.svdi.fr

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LA MÉTHODE



CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Conventions d'écriture pour l'ensemble de ces documents :

- le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [RGPD], par les articles 7 et 8 de la [Charte-UE] et l'article 1 de la [Loi-I&L] : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- l'acronyme « **PIA** » est utilisé pour désigner indifféremment *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

Introduction

Ce guide explique comment mener une "analyse d'impact relative à la protection des données" (cf. art. 35 du [RGPD]), plus communément appelée *Privacy Impact Assessment* (PIA).

Il décrit la manière d'employer la méthode [EBIOS][1] dans le contexte spécifique « Informatique et libertés ». La démarche est conforme aux critères des [LignesDirectrices-G29] (voir la démonstration de couverture fournie en annexe) et compatible avec les normes internationales relatives à la gestion des risques (ex : [ISO 31000]).

Le fonctionnement itératif de cette méthode doit permettre de garantir une utilisation raisonnée et fiable de données à caractère personnel dans le cadre de leur traitement.

La méthode ne traite ni des conditions en amont déterminant s'il faut mener un PIA (cf. art. 35.1 du [RGPD]) ni de celles en aval déterminant qu'il faut consulter l'autorité de protection des données (cf. art. 36.1 du [RGPD]).

Théoriquement mené par un responsable de traitement, un PIA a pour objectif de construire et de démontrer la mise en œuvre des principes de protection de la vie privée afin que les personnes concernées conservent la maîtrise de leurs données à caractère personnel.

Ce guide s'adresse aux responsables de traitements qui souhaitent justifier de leur démarche de conformité et des mesures qu'ils ont choisies (notion de responsabilité ou d'*accountability* en anglais, cf. art. 25 du [RGPD]), ainsi qu'aux fournisseurs de produits qui souhaitent démontrer que leurs solutions sont conçues dans une logique de conception respectueuse de la vie privée (notion de *Privacy by Design* en anglais, cf. art. 25 du [RGPD])[2]. Il est utile à toutes les parties prenantes dans la création ou l'amélioration de traitements de données à caractère personnel ou de produits :

- les autorités décisionnaires, qui commanditent et valident la création de nouveaux traitements de données à caractère personnel ou produits ;
- les maîtrises d'ouvrage, qui doivent apprécier les risques pesant sur leur système et donner des objectifs de sécurité ;
- les maîtrises d'œuvre, qui doivent proposer des solutions pour traiter les risques conformément aux objectifs identifiés par les maîtrises d'ouvrage ;
- les correspondants « informatique et libertés » ou délégués à la protection des données, qui doivent accompagner les maîtrises d'ouvrage et les autorités décisionnaires dans la protection des données à caractère personnel ;
- les responsables de la sécurité des systèmes d'information, qui doivent accompagner les maîtrises d'ouvrage dans le domaine de la sécurité des systèmes d'information.

[1] EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – est la méthode de gestion des risques publiée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).
[2] Dans la suite du document, le terme « traitement de données à caractère personnel » est interchangeable avec le terme « produit ».

Comment mener un PIA ?

La démarche de conformité mise en œuvre en menant un PIA repose sur deux piliers :

1. **les principes et droits fondamentaux**[3], « non négociables », qui sont fixés par la loi et doivent être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. **la gestion des risques sur la vie privée**[4], qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données[5].

Figure 1 – La démarche de conformité à l'aide d'un PIA

En résumé, pour mener un PIA, il convient de :

1. délimiter et décrire le **contexte** du(des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des **principes fondamentaux** : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les **risques** sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. formaliser la **validation** du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

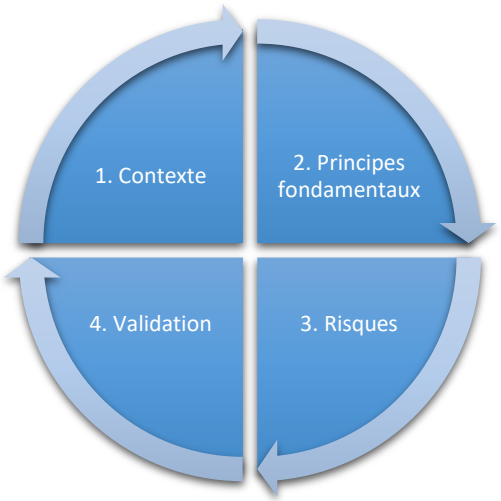


Figure 2 – Démarche générale pour mener un PIA

Il s'agit d'un processus d'amélioration continue. Il requiert donc parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Il requiert en outre une surveillance des évolutions dans le temps (du contexte, des mesures, des risques, etc.), par exemple tous les ans, et des mises à jour dès qu'une évolution significative a lieu.

La démarche devrait être employée dès la conception d'un nouveau traitement de données à caractère personnel. En effet, une application en amont permet de déterminer les mesures nécessaires et suffisantes, et donc d'optimiser les coûts. A contrario, une application tardive, alors que le système est déjà créé et les mesures en place, peut remettre en question les choix effectués.

---

[3] Finalité déterminée, explicite et légitime ; données adéquates, pertinentes et non excessives ; information claire et complète des personnes ; durée de conservation limitée ; droit d'opposition, d'accès, de rectification et suppression, *etc.*

[4] Liés à la sécurité des données à caractère personnel et ayant un impact sur la vie privée des personnes concernées.

[5] Afin de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* » (article 34 de la [Loi-I&L]).

1 Étude du contexte

Généralement réalisée par la maîtrise d'ouvrage[6], avec l'aide d'une personne en charge des aspects « Informatique et libertés »[7].

Objectif : obtenir une vision claire des traitements de données personnelles considérés.

1.1 Vue d'ensemble

- Présenter le **traitement** considéré, sa **nature**, sa **portée**, son **contexte**, ses **finalités** et ses **enjeux**[8] de manière synthétique.
- Identifier le **responsable du traitement** et les éventuels **sous-traitants**.
- Recenser les **référentiels applicables** au traitement, utiles ou à respecter[9], notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD])[10].

1.2 Données, processus et supports

- Délimiter et décrire le périmètre de manière détaillée :
  - les **données** personnelles concernées, leurs **destinataires** et **durées de conservation** ;
  - une description des **processus** et des **supports** de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).

[6] Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.
[7] Correspondant Informatique et libertés, délégué à la protection des données, ou autre.
[8] Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général...) ? ».
[9] Selon les cas, ils serviront notamment à démontrer le respect de principes fondamentaux, à justifier des mesures ou à prouver qu'elles correspondent à l'état de l'art.
[10] Autres exemples : politique de sécurité, normes juridiques sectorielles, etc.

2 Étude des principes fondamentaux

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge des aspects « Informatique et libertés ».

Objectif : bâtir le dispositif de conformité aux principes de protection de la vie privée.

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

- Expliciter et justifier les **choix effectués pour respecter les exigences** suivantes :
  1. **finalité(s)** : déterminée, explicite et légitime (cf. art. 5.1 (b) du [RGPD]) ;
  2. **fondement** : licéité du traitement, interdiction du détournement de finalité (cf. art. 6 du [RGPD])[11] ;
  3. **minimisation des données** : adéquates, pertinentes et limitées (cf. art. 5.1 (c) du [RGPD])[12] ;
  4. **qualité des données** : exactes et tenues à jour (cf. art. 5.1 (d) du [RGPD]) ;
  5. **durées de conservation** : limitées (cf. art. 5.1 (e) du [RGPD]).
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au [RGPD].
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

- Identifier ou déterminer, et décrire, les **mesures retenues** (existantes ou prévues) **pour respecter les exigences** suivantes (nécessitant d'expliquer comment il est prévu de les mettre en œuvre) :
  1. **information** des personnes concernées (traitement loyal et transparent, cf. art. 12, 13 et 14 du [RGPD]) ;
  2. **recueil du consentement**, le cas échéant[13] : exprès, démontrable, retirable (cf. art. 7 et 8 du [RGPD]) ;
  3. exercice des **droits d'accès et à la portabilité** (cf. art. 15 et 20 du [RGPD]);
  4. exercice des **droits de rectification et d'effacement** (cf. art. 16 et 17 du [RGPD])
  5. exercice des **droits de limitation du traitement et d'opposition** (cf. art. 18 et 21 du [RGPD]) ;
  6. **sous-traitance** : identifiée et contractualisée (cf. art. 28 du [RGPD]) ;
  7. **transferts** : respect des obligations en matière de transfert de données en dehors de l'Union européenne (cf. art. 44 à 49 du [RGPD]).
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément au [RGPD].
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

[11] Démontrer également que les destinataires sont légitimes.
[12] Démontrer également que les destinataires ont réellement besoin d'accéder aux données.
[13] Justifier les cas où le consentement n'est pas obtenu.

3 Étude des risques liés à la sécurité des données[14]

Qu'est-ce qu'un risque sur la vie privée ?

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :

- comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- sur les données à caractère personnel (ex. : fichier des clients)
- et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

Le schéma suivant synthétise l'ensemble des notions présentées :

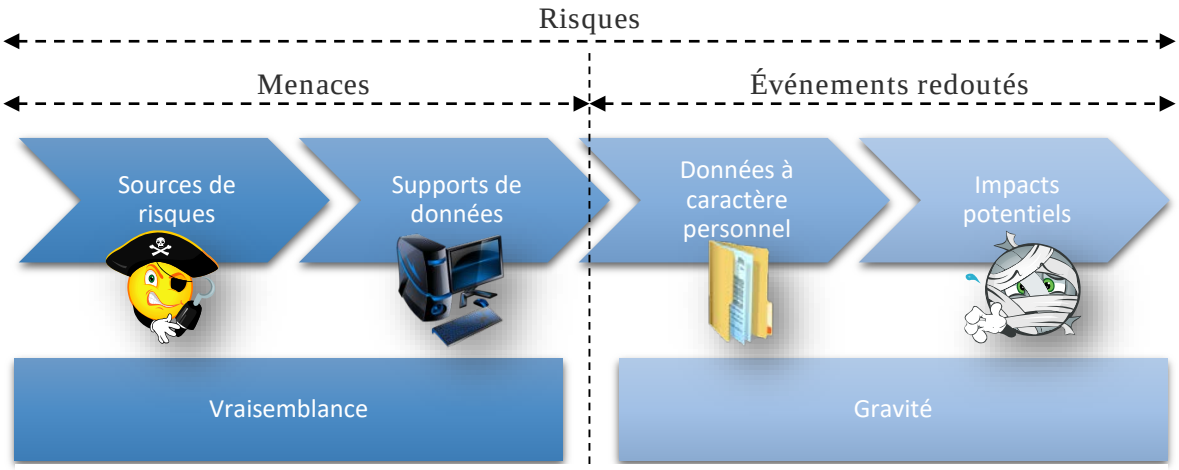


Figure 3 – Éléments composant les risques

Le niveau d'un risque est estimé en termes de gravité et de vraisemblance :

- la **gravité** représente l'ampleur d'un risque. Elle dépend essentiellement du caractère préjudiciable des impacts potentiels[15] ;
- la **vraisemblance** traduit la possibilité qu'un risque se réalise. Elle dépend essentiellement des vulnérabilités des supports face aux menaces et des capacités des sources de risques à les exploiter.

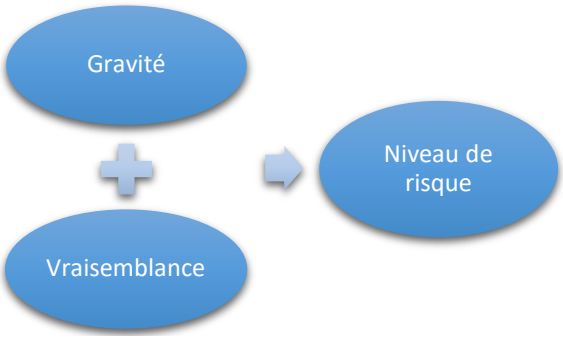


Figure 4 – Éléments permettant d'estimer les risques

[14] Cf. art. 32 du [RGPD].
[15] Compte tenu du contexte (nature des données, personnes concernées, finalité du traitement, etc.).

3.1 Évaluation des mesures existantes ou prévues

Généralement réalisé par la maîtrise d'œuvre[16], puis évaluée par une personne en charge de la sécurité de l'information[17].

Objectif : obtenir une bonne connaissance des mesures contribuant à la sécurité.

- Identifier ou déterminer les **mesures existantes ou prévues** (déjà engagées), qui peuvent être de trois natures différentes :
  1. **mesures portant spécifiquement sur les données du traitement** : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, etc. ;
  2. **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** : sécurité de l'exploitation, sauvegardes, sécurité des matériels, etc. ;
  3. **mesures organisationnelles (gouvernance)** : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, etc.
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.
- Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge de la sécurité de l'information.

Objectif : obtenir une bonne compréhension des causes et conséquences des risques.

- Pour chaque événement redouté (un accès illégitime à des données[18], une modification non désirée de données[19], et une disparition de données[20]) :
  1. déterminer les **impacts** potentiels sur la vie privée des personnes concernées s'ils survenaient[21] ;
  2. estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
  3. identifier les **menaces** sur les supports des données qui pourraient mener à cet événement redouté[22] et les **sources de risques** qui pourraient en être à l'origine ;
  4. estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.
- Déterminer si les risques ainsi identifiés[23] peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.
- Dans la négative, proposer des mesures complémentaires et ré-estimer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels.

[16] Elle peut être déléguée, représentée ou sous-traitée.
[17] Responsable de la sécurité des systèmes d'information ou autre.
[18] Elles sont connues de personnes non autorisées (atteinte à la confidentialité des données).
[19] Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des données).
[20] Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des données).
[21] Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».
[22] Répondre à la question « Comment cela pourrait-il arriver ? ».
[23] Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.

4 Validation du PIA

Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés ».

Objectif : décider d'accepter ou non le PIA au regard des résultats de l'étude.

4.1 Préparation des éléments utiles à la validation

- Consolider et mettre en forme les résultats de l'étude :
  1. élaborer une représentation visuelle des **mesures choisies pour respecter les principes fondamentaux,** en fonction de leur conformité au [RGPD] (ex : à améliorer, ou jugé comme conforme) ;
  2. élaborer une représentation visuelle des **mesures choisies pour contribuer à la sécurité des données**, en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;
  3. élaborer une cartographie visuelle des **risques résiduels**[24] en fonction de leur gravité et vraisemblance ;
  4. élaborer un **plan d'action** à partir des mesures complémentaires identifiées lors des étapes précédentes : pour chaque mesure, déterminer au moins le responsable de sa mise en œuvre, son coût (financier et/ou en termes de charge) et son échéance prévisionnelle.
- Formaliser la prise en compte des parties prenantes :
  1. le **conseil de la personne en charge des aspects « Informatique et libertés »**, si elle a été désignée (cf. art. 35 (2) du [RGPD]) ;
  2. l'**avis des personnes concernées ou de leurs représentants**, le cas échéant (cf. art. 35 (9) du [RGPD]).

4.2 Validation formelle

- Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être :
  1. validé ;
  2. à améliorer (expliquer en quoi) ;
  3. refusé (ainsi que le traitement considéré).
- Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé.

[24] Risques qui subsistent après application des mesures.

Annexes

Définitions

Note : les libellés entre parenthèses correspondent aux libellés courts employés dans ce document.

Donnée à caractère personnel (donnée)

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. [RGPD]

Note : 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. [Loi-I&L]

Événement redouté

Violation potentielle de données pouvant mener à des impacts sur la vie privée des personnes concernées.

Gravité

Estimation de l'ampleur des impacts potentiels sur la vie privée des personnes concernées.

Note : elle dépend essentiellement du caractère préjudiciable des impacts potentiels.

Menace

Mode opératoire composé d'une ou plusieurs actions unitaires sur des supports de données.

Note : elle est utilisée, volontairement ou non, par des sources de risques, et peut provoquer un événement redouté.

Mesure

Action à entreprendre.

Note : elle peut être technique ou organisationnelle, et peut consister mettre en œuvre des principes fondamentaux ou à éviter, réduire, transférer ou prendre tout ou partie des risques.

Personnes concernées

Personnes auxquelles se rapportent les données qui font l'objet du traitement. [Loi-I&L]

Responsable de traitement

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. [RGPD]

Note : sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement. [Loi-I&L]

Risque

Scénario décrivant un événement redouté et toutes les menaces qui le rendent possibles.

	Note : il est estimé en termes de gravité et de vraisemblance.
Source de risque	Personne ou source non humaine qui peut être à l'origine d'un risque. *Note : elle peut agir de manière accidentelle ou délibérée.*
Support de données	Bien sur lequel reposent des données. *Note : il peut s'agir de matériels, de logiciels, de canaux informatiques, de personnes, de supports papier ou de canaux de transmission papier.*
Traitement de données à caractère personnel (traitement)	Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction. [RGPD]
Vraisemblance	Estimation de la possibilité qu'un risque se réalise. *Note : elle dépend essentiellement des vulnérabilités exploitables et des capacités des sources de risques à les exploiter.*

Références bibliographiques

[Charte-UE]	Charte des droits fondamentaux de l'Union européenne, 2010/C 83/02.
[RGPD]	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).
[Loi-I&L]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée[25].
[LignesDirectrices-G29]	Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248 rév. 01, Groupe de travail « Article 29 » sur la protection des données.
[EBIOS]	Expression des Besoins et Identification des Objectifs de Sécurité – EBIOS – Méthode de gestion des risques, ANSSI.
[ISO 31000]	ISO 31000:2009, Management du risque – Principes et lignes directrices, ISO.

[25] Modifiée par la 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 et par la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures.

Couverture des critères des [LignesDirectrices-G29]

Critères des [LignesDirectrices-G29] (et références au [RGPD])	Couverture	Chapitre de ce guide
Une description systématique du traitement est fournie (Article 35(7)(a)) : - la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90) ; - les données à caractère personnel, destinataires et durée de conservation sont recensés ; - une description fonctionnelle du traitement est fournie ; - les biens sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, papier ou canaux de transmission papier) sont identifiés ; - la conformité à des codes de conduite approuvés est prise en compte (Article 35(8)).	☑	1. Étude du contexte

La nécessité et la proportionnalité sont évaluées (Article 35(7)(b)) :
- les mesures envisages pour se conformer au Règlement sont déterminées (Article 35(7)(d) et considérant 90) en tenant compte :
  - des mesures contribuant à la proportionnalité et à la nécessité du traitement, sur la base de :
  - une(des) finalité(s) déterminée(s), explicite(s) et légitime(s) (Article 5(1)(b));
  - la licéité du traitement (Article 6);
  - des données adéquates, pertinentes et limitées à ce qui est nécessaire (Article 5(1)(c));
  - une durée de conservation limitée (Article 5(1)(e));
  - des mesures contribuant aux droits des personnes concernées :
  - l'information des personnes concernées (Articles 12, 13 et 14);
  - le droit d'accès et à la portabilité (Articles 15 et 20) ;
  - les droits de rectification et à l'effacement (Articles 16 et 17);
  - les droits d'opposition et à la limitation du traitement (Articles 16 et 21);
  - les sous-traitants (Article 28);
  - les mesures encadrant le(s) transfert(s) internationaux (Chapitre V).
	☑	2. Étude des principes fondamentaux

Les risques sur les droits et libertés des personnes concernées sont gérés (Article 35(7)(c)):
- l'origine, la nature, la particularité et la gravité des risques sont appréciées (cf. considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime, modification non désirée et disparition de données), du point de vue des personnes concernées :
  - les sources de risques sont prises en compte (considérant 90) ;
  - les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'accès illégitime, de modification on désirée et de disparition de données ;
  - les menaces qui pourraient mener à un accès illégitime, une modification non désirée et une disparition de données sont identifiées ;
  - la vraisemblance et la gravité sont estimées (considérant 90) ;
- les mesures envisagées pour traiter ces risques sont déterminées (Article 35(7)(d) et considérant 90).
	☑	3. Étude des risques liés à la sécurité des données

Les parties intéressées sont impliquées : - le conseil du délégué à la protection des données est demandé (Article 35(2)) ; - l'avis des personnes concernées ou de leurs représentants sont demandés (Article 35(9)).	☑	4. Validation du PIA

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LES MODÈLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Avant-propos

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Conventions d'écriture pour l'ensemble de ces documents :

- le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [RGPD], par les articles 7 et 8 de la [Charte-UE] et l'article 1 de la [Loi-I&L] : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- l'acronyme « **PIA** » est utilisé pour désigner indifféremment *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

Attention : les bases de connaissances présentées dans ce guide constituent une aide à la mise en œuvre de la démarche. Il est tout à fait possible et même souhaitable de les adapter à chaque contexte particulier.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

1 Modèles utiles à l'étude du contexte

1.1 Vue d'ensemble

Présentation du(des) traitement(s) considéré(s)

Description du traitement[1]	
Finalités du traitement	
Enjeux du traitement	
Responsable du traitement	
Sous-traitant(s)	

Recensement des référentiels applicables au traitement[2]

Référentiels applicables au traitement	Prise en compte

1.2 Données, processus et supports

Description des données, destinataires et durées de conservation

Données	Destinataires	Durées de conservation

Description des processus et supports

[insérer un schéma des flux de données et la description détaillée des processus mis en œuvre]

Processus	Description détaillée du processus	Supports des données concernés

[1] Sa nature, sa portée, son contexte, *etc.*
[2] Voir article 35 (8) du [RGPD].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

2 Modèles utiles à l'étude des principes fondamentaux

2.1 Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

Explication et justification des finalités

Finalités	Légitimité

Explication et justification du fondement

Critères de licéité	Applicable	Justification
La personne concernée a consenti[3] au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques		
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci		
Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis		
Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique		
Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement		
Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[4]		

[3] Concernant le recueil du consentement de la personne et son information, voir le 2.2.
[4] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Explication et justification de la minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation

Explication et justification de la qualité des données

Mesures pour la qualité des données	Justification

Explication et justification des durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données courantes			
Données archivées			
Traces fonctionnelles			
Journaux techniques (logs)			

Évaluation des mesures

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable ?	Mesures correctives
Finalités : déterminées, explicites et légitimes		
Fondement : licéité du traitement, interdiction du détournement de finalité		
Minimisation des données : adéquates, pertinentes et limitées		
Qualité des données : exactes et tenues à jour		
Durées de conservation : limitées		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

2.2 Évaluation des mesures protectrices des droits des personnes des personnes concernées

Détermination et description des mesures pour l'information des personnes

Si le traitement bénéficie d'une exemption au droit d'information, prévue par l'article 32 de la [Loi-I&L] et les articles 12, 13 et 14 du [RGPD] :

Dispense d'information des personnes concernées	Justification

Dans le cas contraire :

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Présentation des conditions d'utilisation/confidentialité		
Possibilité d'accéder aux conditions d'utilisation/confidentialité		
Conditions lisibles et compréhensibles		
Existence de clauses spécifiques au dispositif		
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)		
Présentation détaillée des données personnelles collectées		
Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers		
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)		
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation		
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité		
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures pour le droit à l'information	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Dans le cas de transmission de données à des tiers :		
- présentation détaillée des finalités de transmission à des tiers		
- présentation détaillée des données personnelles transmises		
- indication de l'identité des entreprises tierces		

Détermination et description des mesures pour le recueil du consentement[5]

Mesures pour le recueil du consentement	Modalités de mise en œuvre	Justification des modalités ou de l'impossibilité de leur mise en œuvre
Consentement exprès à l'inscription		
Consentement segmenté par catégorie de données ou types de traitement		
Consentement exprès avant le partage de données avec des tiers		
Consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants)		
Recueil du consentement des parents pour les mineurs de moins de 13 ans		
Pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement		
Après une longue période sans utilisation, demande à la personne concernée de réaffirmer son consentement		
Si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface signale clairement que ce traitement a lieu (icône, voyant lumineux)		
Si l'utilisateur change de contrat, les paramètres liés à son consentement sont maintenus		

Détermination et description des mesures pour les droits d'accès et à la portabilité

[5] Si la licéité du traitement repose sur le consentement.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Si le traitement bénéficie d'une exemption au droit d'accès, prévue par les articles 39 et 41 de la loi [Loi-I&L] et les articles 15 et 20 du [RGPD] :

Exemption du droit d'accès	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour le droit d'accès	Données internes	Données externes	Justification
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes			
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à la personne concernée			
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à la personne concernée			

Enfin, quand le droit à la portabilité est applicable au traitement prévu par l'article 20 du [RGPD] :

Mesures pour le droit à la portabilité	Données internes	Données externes	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par la personne concernée, afin de pouvoir les transférer à un service tiers			

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de rectification et d'effacement

Si le traitement bénéficie d'une exemption au droit de rectification et d'effacement, prévue par l'article 41 de la [Loi-I&L] et l'article 17 du [RGPD] :

Exemption des droits de rectification et d'effacement	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour les droits de rectification et d'effacement	Données internes	Données externes	Justification
Possibilité de rectifier les données personnelles			
Possibilité de supprimer les données personnelles			
Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, etc.)			
Mise en œuvre du droit à l'oubli pour les mineurs			
Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut			
Conseils fournis pour remise à zéro en cas de vente de l'appareil			
Possibilité d'effacer les données en cas de vol de l'appareil			

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour les droits de limitation du traitement et d'opposition

Si le traitement bénéficie d'une exemption au droit de limitation et d'opposition, prévue par l'article 38 de la [Loi-I&L] ou l'article 21 du [RGPD] :

Exemption des droits de limitation et d'opposition	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire :

Mesures pour les droits de limitation et d'opposition	Données internes	Données externes	Justification
Existence de paramètres « Vie privée »			
Invitation à changer les paramètres par défaut			
Paramètres « Vie privée » accessibles pendant l'inscription			
Paramètres « Vie privée » accessibles après l'inscription			
Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans			
Conformité en matière de traçage (Cookies, Publicité, etc.)			
Exclusion des enfants de moins de 13 ans des traitements de profilage automatisé			
Exclusion effective de traitement des données de l'utilisateur en cas de retrait du consentement			

Détermination et description des mesures pour la sous-traitance

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28[6]

[6] Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'art. 28 du [RGPD] : durée, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du [RGPD], notification immédiate de toute violation de données, *etc.*

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne

Données	France	UE	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)

Évaluation des mesures

Mesures protectrices des droits des personnes concernées	Acceptable / améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)		
Recueil du consentement		
Exercice des droits d'accès et à la portabilité		
Exercice des droits de rectification et d'effacement		
Exercice des droits de limitation du traitement et d'opposition		
Sous-traitance : identifiée et contractualisée		
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

3 Modèles utiles à l'étude des risques liés à la sécurité des données

3.1 Évaluation des mesures

Description et évaluation des mesures contribuant à traiter des risques liés à la sécurité des données

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Chiffrement	[*Décrivez ici les moyens mis en œuvre pour assurer la confidentialité des données conservées (en base de données, dans des fichiers plats, les sauvegardes, etc.), ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).* *Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) mis en œuvre dans le traitement.*]		
Anonymisation	[*Indiquez ici si des mécanismes d'anonymisation sont mis en œuvre, lesquels et à quelle fin.*]		
Cloisonnement des données (par rapport au reste du système d'information)	[*Indiquez ici si un cloisonnement du traitement est prévu, et comment il est réalisé.*]		
Contrôle des accès logiques	[*Indiquez ici comment les profils utilisateurs sont définis et attribués.* *Précisez les moyens d'authentification mis en œuvre*[7]. *Le cas échéant, précisez les*		

[7] Voir la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures portant spécifiquement sur les données du traitement	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	règles applicables aux mots de passe (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).]		
Traçabilité (journalisation)	[*Indiquez ici si des événements sont journalisés et la durée de conservation de ces traces.*]		
Contrôle d'intégrité	[*Indiquez ici si des mécanismes de contrôle d'intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin.* *Détaillez les mécanismes de contrôle d'intégrité employés sur les flux de données.*]		
Archivage	[*Décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d'archivage (service producteur, service versant, etc.) et la politique d'archivage.* *Indiquez si les données sont susceptibles de relever des archives publiques.*]		
Sécurité des documents papier	[*Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures générales de sécurité

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Sécurité de l'exploitation	[*Décrivez ici comment les mises à jour des logiciels (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.*]		
Lutte contre les logiciels malveillants	[*Précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.*]		
Gestion des postes de travail	[*Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.).*]		
Sécurité des sites web	[*Indiquez ici si les "recommandations pour la sécurisation des sites web" de l'ANSSI sont mises en œuvre.*]		
Sauvegardes	[*Indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.*]		
Maintenance	[*Décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée.* *Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités.* *Précisez si les matériels défectueux sont gérés spécifiquement.*]		
Sécurité des canaux informatiques (réseaux)	[*Indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet).* *Précisez quels système de pare-feu, sondes de*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.]		
Surveillance	[*Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens.* *Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.*]		
Contrôle d'accès physique	[*Indiquez ici la manière dont est réalisé le contrôle d'accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.).* *Indiquez s'il existe des moyens d'alerte en cas d'effraction.*]		
Sécurité des matériels	[*Indiquez ici les mesures de sécurité physique des serveurs et des postes clients (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.).*]		
Éloignement des sources de risques	[*Indiquez ici si la zone d'implantation est sujette à des sinistres environnementaux (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc.)* *Précisez si la zone contient des produits dangereux.*]		
Protection contre les sources de risques non humaines	[*Décrivez ici les moyens de prévention, de détection et de lutte contre l'incendie.* *Le cas échéant, indiquez les*		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
	moyens de prévention de dégâts des eaux. *Précisez également les moyens de surveillance et de secours de l'alimentation électrique.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Description et évaluation des mesures organisationnelles (gouvernance)

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Organisation	[*Indiquez si les rôles et responsabilités en matière de protection des données sont définis.* *Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée.* *Précisez s'il existe un comité de suivi (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.*]		
Politique (gestion des règles)	[*Indiquez ici s'il existe une charte informatique (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques.*]		
Gestion des risques	[*Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode.* *Précisez s'il existe, au niveau de l'organisme, une cartographie des risques sur la vie privée.*]		
Gestion des projets	[*Indiquez ici si les tests des dispositifs sont réalisés sur des données fictives/anonymes.*]		
Gestion des incidents et des violations de données	[*Indiquez ici si les incidents font l'objet d'une gestion documentée et testée, notamment en ce qui concerne les violations de données à caractère personnel.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Mesures organisationnelles (gouvernance)	Modalités de mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Gestion des personnels	[*Indiquez ici les mesures de sensibilisation prises à l'arrivée d'une personne dans sa fonction.* *Indiquez les mesures prises au départ des personnes accédant aux données.*]		
Relations avec les tiers	[*Indiquez ici, notamment pour les sous-traitants amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.*]		
Supervision	[*Indiquez ici si l'effectivité et l'adéquation des mesures touchant à la vie privée sont contrôlées.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

Analyse et estimation des risques

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

Évaluation des risques

Risques	Acceptable / améliorable ?	Mesures correctives	Gravité résiduelle	Vraisemblance résiduelle
Accès illégitime à des données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Modification non désirée de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		
Disparition de données	[*L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.*]	[*Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.*]		

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4 Modèles utiles à la validation du PIA

4.1 Préparation des éléments utiles à la validation

Élaboration de la synthèse relative à la conformité au [RGPD] des mesures permettant de respecter les principes fondamentaux

Légende				
Symbole :	●●●	●○○	○●○	○○●
Signification :	Non applicable	Insatisfaisant	Amélioration prévue	Satisfaisant

Mesures permettant de respecter les principes fondamentaux	Évaluation
Mesures garantissant la proportionnalité et la nécessité du traitement	
Finalités : déterminées, explicites et légitimes	○○○
Fondement : licéité du traitement, interdiction du détournement de finalité	○○○
Minimisation des données : adéquates, pertinentes et limitées	○○○
Qualité des données : exactes et tenues à jour	○○○
Durées de conservation : limitées	○○○
Mesures protectrices des droits des personnes des personnes concernées	
Information des personnes concernées (traitement loyal et transparent)	○○○
Recueil du consentement	○○○
Exercice des droits d'accès et à la portabilité	○○○
Exercice des droits de rectification et d'effacement	○○○
Exercice des droits de limitation du traitement et d'opposition	○○○
Sous-traitance : identifiée et contractualisée	○○○
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	○○○

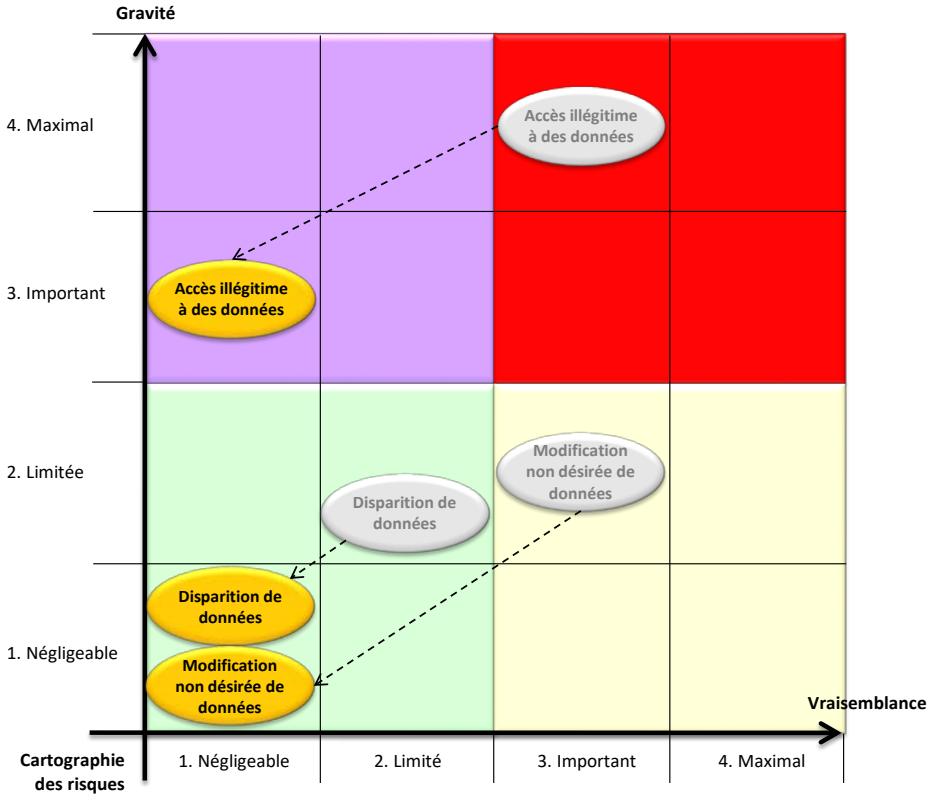
Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures des mesures contribuant à traiter les risques liés à la sécurité des données

Mesures contribuant à traiter les risques liés à la sécurité des données	Évaluation
Mesures portant spécifiquement sur les données du traitement	
Chiffrement	○○○
Anonymisation	○○○
Cloisonnement des données (par rapport au reste du système d'information)	○○○
Contrôle des accès logiques des utilisateurs	○○○
Traçabilité (journalisation)	○○○
Contrôle d'intégrité	○○○
Archivage	○○○
Sécurité des documents papier	○○○
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	
Sécurité de l'exploitation	○○○
Lutte contre les logiciels malveillants	○○○
Gestion des postes de travail	○○○
Sécurité des sites web	○○○
Sauvegardes	○○○
Maintenance	○○○
Sécurité des canaux informatiques (réseaux)	○○○
Surveillance	○○○
Contrôle d'accès physique	○○○
Sécurité des matériels	○○○
Éloignement des sources de risques	○○○
Protection contre les sources de risques non humaines	○○○
Mesures organisationnelles (gouvernance)	
Organisation	○○○
Politique (gestion des règles)	○○○
Gestion des risques	○○○
Gestion des projets	○○○
Gestion des incidents et des violations de données	○○○
Gestion des personnels	○○○
Relations avec les tiers	○○○
Supervision	○○○

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration de la cartographie des risques liés à la sécurité des données



Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Élaboration du plan d'action

Mesures complémentaires demandées	Responsable	Terme	Difficulté	Coût	Avancement

Formalisation du conseil de la personne en charge des aspects « Informatique et libertés »[8]

Le [jj/mm/aaaa], le délégué à la protection des données de [nom de l'organisme] a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

[Signature]

Formalisation de l'avis des personnes concernées ou de leurs représentants[9]

Les personnes concernées [ont/n'ont pas été] consultées [et ont émis l'avis suivant sur la conformité du traitement au vu du PIA mené] :

Justification de la décision du responsable de traitement :

[8] Voir l'article 35 (2) du [RGPD].
[9] Voir l'article 35 (9) du [RGPD].

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

4.2 Validation formelle

Formalisation de la validation

Le [jj/mm/aaaa], le [poste du responsable de traitement] de [nom de l'organisme] valide le PIA du traitement [nom du PIA], au vu du PIA mené, en sa qualité de responsable du traitement.

Le traitement a pour finalité de [rappel de la finalité du traitement].

Les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques sur la vie privée des personnes concernées sont en effet jugées acceptables au regard de cet enjeu. La mise en œuvre des mesures complémentaires devra toutefois être démontrée, ainsi que l'amélioration continue du PIA.

[Signature]

Attention : ces modèles et bases de connaissances peuvent devoir être adaptés, et devraient être utilisés en support du guide "PIA, la méthode".

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

LES BASES DE CONNAISSANCES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos

La méthode de la CNIL est composée de trois guides, décrivant respectivement la démarche, des modèles utiles pour formaliser l'étude et des bases de connaissances (un catalogue de mesures destinées à respecter les exigences légales et à traiter les risques, et des exemples) utiles pour mener l'étude :

Ils sont téléchargeables sur le site de la CNIL :

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Conventions d'écriture pour l'ensemble de ces documents :

- le terme « **vie privée** » est employé comme raccourci pour évoquer l'ensemble des libertés et droits fondamentaux (notamment ceux évoqués dans le [RGPD], par les articles 7 et 8 de la [Charte-UE] et l'article 1 de la [Loi-I&L] : « vie privée, identité humaine, droits de l'homme et libertés individuelles ou publiques ») ;
- l'acronyme « **PIA** » est utilisé pour désigner indifféremment *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données, et *Data Protection Impact Assessment* (DPIA) ;
- les libellés entre crochets ([libellé]) correspondent aux références bibliographiques.

1 Bases de connaissances utiles à l'étude

1.1 Typologie de données à caractère personnel

Les catégories de données sont généralement les suivantes :

Types de données	Catégories de données
DCP courantes	État-civil, identité, données d'identification
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses...)
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions...)
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale...)
	Données de connexion (adresses IP, journaux d'événements...)
	Données de localisation (déplacements, données GPS, GSM...)
DCP perçues comme sensibles	Numéro de sécurité sociale (NIR)
	Données biométriques
	Données bancaires
DCP sensibles au sens de la [Loi-I&L][1]	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle
	Infractions, condamnations, mesures de sécurité

Notes

- Les supports des données peuvent être regroupés en ensembles cohérents.

1.2 Typologie de supports de données

Les supports de données sont les composants du système d'information sur lesquels reposent les données à caractère personnel :

Types de supports de données		Exemples
Systèmes informatiques	Matériels et supports de données électroniques	Ordinateurs, relais de communication, clés USB, disques durs
	Logiciels	Systèmes d'exploitation, messagerie, bases de données, applications métier
	Canaux informatiques	Câbles, WiFi, fibre optique
Organisations	Personnes	Utilisateurs, administrateurs informatiques, décideurs
	Supports papier	Impressions, photocopies, documents manuscrits
	Canaux de transmission papier	Envoi postal, circuit de validation

Notes

- Il convient de choisir le niveau de détail le plus approprié au sujet de l'étude.
- Les solutions de sécurité (produits, procédures, mesures...) ne sont pas des supports de données : il s'agit de mesures destinées à traiter les risques.

[1] Voir notamment les articles 8 et 9 de la [Loi-I&L] et l'article 8 de la [Directive-95-46].

1.3 Typologie de sources de risques

Le tableau suivant présente des exemples de sources de risques :

Types de sources de risques	Exemples
Sources humaines internes	Salariés, administrateurs informatiques, stagiaires, dirigeants
Sources humaines externes	Destinataires des DCP, tiers autorisés[2], prestataires, pirates informatiques, visiteurs, anciens employés, militants, concurrents, clients, personnels d'entretien, maintenance, délinquant, syndicats, journalistes, organisations non gouvernementales, organisations criminelles, organisations sous le contrôle d'un État étranger, organisations terroristes, activités industrielles environnantes
Sources non humaines	Codes malveillants d'origine inconnue (virus, vers...), eau (canalisations, cours d'eau...), matières inflammables, corrosives ou explosives, catastrophes naturelles, épidémies, animaux

1.4 Échelle et règles pour estimer la gravité

La gravité représente l'ampleur d'un risque. Elle est essentiellement estimée au regard de la hauteur des impacts potentiels sur les personnes concernées, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la gravité des événements redoutés (**attention : ce ne sont que des exemples, qui peuvent être très différents selon le contexte**) :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) - Maux de tête passagers	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : spams) - Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) - Publicité ciblée pour des produits de consommation courants	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données - Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) - Perte de temps pour paramétrer ses données - Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)

[2] Par exemple, des autorités publiques et auxiliaires de justice peuvent demander communication de certaines données quand la loi les y autorise expressément.
[3] Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique.
[4] Perte subie ou gain manqué concernant le patrimoine des personnes.
[5] Souffrance physique ou morale, préjudice esthétique ou d'agrément.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales - Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) - Promotion professionnelle manquée - Compte à des services en ligne bloqué (ex. : jeux, administration) - Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées - Élévation de coûts (ex. : augmentation du prix d'assurance) - Données non mises à jour (ex. : poste antérieurement occupé) - Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) - Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) - Profilage imprécis ou abusif	- Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) - Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) - Sentiment d'atteinte à la vie privée sans préjudice irrémédiable - Intimidation sur les réseaux sociaux
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	- Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre-indications) - Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	- Détournements d'argent non indemnisé - Difficultés financières non temporaires (ex. : obligation de contracter un prêt) - Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) - Interdiction bancaire - Dégradation de biens - Perte de logement - Perte d'emploi - Séparation ou divorce - Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - phishing) - Bloqué à l'étranger	- Affection psychologique grave (ex. : dépression, développement d'une phobie) - Sentiment d'atteinte à la vie privée et de préjudice irrémédiable - Sentiment de vulnérabilité à la suite d'une assignation en justice - Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) - Victime de chantage - Cyberbullying et harcèlement moral

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[3]	Exemples d'impacts matériels[4]	Exemples d'impacts moraux[5]
			- Perte de données clientèle	
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	- Affection physique de longue durée ou permanente (ex. : suite au non respect d'une contre-indication) - Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l'intégrité physique	- Péril financier - Dettes importantes - Impossibilité de travailler - Impossibilité de se reloger - Perte de preuves dans le cadre d'un contentieux - Perte d'accès à une infrastructure vitale (eau, électricité)	- Affection psychologique de longue durée ou permanente - Sanction pénale - Enlèvement - Perte de lien familial - Impossibilité d'ester en justice - Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

On retient la valeur dont la description correspond le mieux aux impacts potentiels identifiés, en comparant les impacts identifiés dans le contexte considéré avec les impacts génériques de l'échelle.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- le caractère identifiant des données ;
- la nature des sources de risques ;
- le nombre d'interconnexions (notamment avec l'étranger) ;
- le nombre de destinataires (ce qui facilite la corrélation de données initialement séparées).

1.5 Échelle et règles pour estimer la vraisemblance

La vraisemblance traduit la possibilité qu'un risque se réalise. Elle est essentiellement estimée au regard des vulnérabilités des supports concernés et de la capacité des sources de risques à les exploiter, compte tenu des mesures existantes, prévues ou complémentaires (qu'il convient de mentionner en tant que justification).

L'échelle suivante peut être utilisée pour estimer la vraisemblance des menaces :

1. Négligeable : il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

On retient la valeur dont la description correspond le mieux aux vulnérabilités des supports et aux sources de risques identifiés.

Elle peut être augmentée ou diminuée en fonction d'autres facteurs, tels que les suivants :

- une ouverture sur Internet ou un système fermé ;
- des échanges de données avec l'étranger ou non ;
- des interconnexions avec d'autres systèmes ou aucune interconnexion ;
- l'hétérogénéité ou l'homogénéité du système ;
- la variabilité ou la stabilité du système ;
- l'image de l'organisme.

1.6 Menaces qui peuvent mener à un accès illégitime à des données

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
C	Matériels	Utilisés de manière inadaptée	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles, le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.)	Utilisable en dehors de l'usage prévu, disproportion entre le dimensionnement des matériels et le dimensionnement nécessaire (par exemple : disque dur de plusieurs To pour stocker quelques Go de données)
C	Matériels	Observés	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance	Permet d'observer des données interprétables, émet des signaux compromettants
C	Matériels	Modifiés	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
C	Matériels	Perdus	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique	Petite taille, attractif (valeur marchande)
C	Logiciels	Utilisés de manière inadaptée	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
C	Logiciels	Observés	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source
C	Logiciels	Modifiés	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés)	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
C	Canaux informatiques	Observés	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables
C	Personnes	Observées	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle	Peu discret (loquace, sans réserve), routinier (habitudes facilitant l'espionnage récurrent)
C	Personnes	Détournées	Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral)	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté), manipulable (vulnérable aux pressions sur soi ou son entourage)

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
C	Personnes	Perdues	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
C	Documents papier	Observés	Lecture, photocopie, photographie	Permet d'observer des données interprétables
C	Documents papier	Perdus	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut	Portable
C	Canaux papier	Observés	Lecture de parapheurs en circulation, reproduction de documents en transit	Observable

1.7 Menaces qui peuvent mener à une modification non désirées de données

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
I	Matériels	Modifiés	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
I	Logiciels	Utilisés de manière inadaptée	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
I	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
I	Canaux informatiques	Utilisés de manière inadaptée	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds)
I	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement
I	Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
I	Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
I	Canaux papier	Modifiés	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier

1.8 Menaces qui peuvent mener à une disparition de données

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
D	Matériels	Utilisés de manière inadaptée	Stockage de fichiers personnels, utilisation à des fins personnelles	Utilisable en dehors de l'usage prévu
D	Matériels	Surchargés	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par dénis de service	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension
D	Matériels	Modifiés	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
D	Matériels	Détériorés	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires)
D	Matériels	Perdus	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel, disques sous dimensionnés amenant à une multiplication des supports et à la perte de certains	Portable, attractif (valeur marchande)
D	Logiciels	Utilisés de manière inadaptée	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
D	Logiciels	Surchargés	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues, attaque par dénis de service	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable
D	Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
D	Logiciels	Détériorés	Effacement d'un exécutable en production ou de code sources, virus, bombe logique	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications)
D	Logiciels	Perdus	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données, arrêt des mises à jour de maintenance de sécurité par l'éditeur, faillite de l'éditeur, corruption du module de stockage contenant les numéros de licence	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne), attractif (rare, novateur, grande valeur commerciale), cessible (clause de cessibilité totale dans la licence)
D	Canaux informatiques	Surchargés	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée)
D	Canaux informatiques	Détériorés	Sectionnement de câblage, mauvaise réception du réseau wifi, oxydation des câbles	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné), unique

Critères touché	Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
D	Canaux informatiques	Perdus	Vol de câbles de transmission en cuivre	Attractif (valeur marchande des câbles), transportable (léger, dissimulable), peu visible (oubliable, insignifiant, peu remarquable)
D	Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement
D	Personnes	Détériorées	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales
D	Personnes	Perdues	Décès, retraite, changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
D	Documents papier	Utilisés de manière inadaptée	Effacement progressif avec le temps, effacement volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, pour faire la liste de course, utilisation des cahiers pour faire autre chose	Modifiable (support papier au contenu effaçable, papiers thermiques non résistants aux modifications de températures)
D	Documents papier	Détériorés	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation
D	Documents papier	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable
D	Canaux papier	Surchargés	Surcharge de courriers, surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives
D	Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique
D	Canaux papier	Modifiés	Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation de circuits papier, changement de langue professionnelle	Modifiable (remplaçable)
D	Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de postes	Utilité non reconnue

1.9 Échelles pour le plan d'action

Les échelles suivantes peuvent être utilisées pour élaborer le plan d'action et suivre sa mise en œuvre :

Critère	Niveau 1	Niveau 2	Niveau 3
Difficulté	Faible	Moyenne	Élevée
Coût financier	Nul	Moyen	Important
Terme	Trimestre	Année	3 ans
Avancement	Non démarré	En cours	Terminé

2 Anonymisation

Objectifs : faire perdre le caractère identifiant des données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Déterminer ce qui doit être anonymisé selon le contexte, la forme de stockage des données (champs d'une base de données, extraits de textes, etc.) et les risques identifiés.
- Anonymiser de manière irréversible ce qui doit l'être, selon la forme des données à anonymiser (base de données, documents textuels, etc.) et les risques identifiés.
- Si ce qui doit être anonymisé ne peut l'être de manière irréversible, choisir les outils (suppression partielle, chiffrement, hachage, hachage à clé, index, etc.) qui satisfont le mieux possible les besoins fonctionnels.

3 Archivage

Objectifs : définir l'ensemble des modalités de conservation et gestion d'archives électroniques contenant des données à caractère personnel destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire (versement, stockage, migration, accessibilité, élimination, politique d'archivage, protection de la confidentialité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les processus de gestion des archives sont définis.
  - ♦ *Recommandations : distinguer les processus de versement, stockage, gestion des données descriptives, consultation/communication et administration (relation avec les services producteurs, veille technologique et juridique, projets d'évolution et migration des supports et des formats).*
- Vérifier que les rôles en matière d'archivage sont identifiés.
  - ♦ *Recommandations : distinguer les services producteurs, services versants, autorités d'archivage (responsables de la conservation), services contrôleurs (exerçant le contrôle scientifique et technique sur les archives publiques).*
- Vérifier que les mesures prises permettent de garantir, si besoin, l'identification et l'authentification de l'origine des archives, l'intégrité des archives, l'intelligibilité et la lisibilité des archives, la durée de conservation des archives, la traçabilité des opérations effectuées sur les archives (versement, consultation, migration, élimination, etc.), la disponibilité et l'accessibilité des archives, les compléter si ce n'est pas le cas.
  - ♦ *Recommandations : mettre en œuvre des modalités d'accès spécifiques aux données archivées, chiffrer les archives et prévoir de les re-chiffrer de manière sécurisée avec de nouvelles clés avant la fin de vie des clés de chiffrement, prévoir le changement des supports obsolètes des données, choisir un mode opératoire de destruction des archives garantissant que l'intégralité a été détruite?*
- Déterminer les moyens de protection de la confidentialité des données archivées selon les risques identifiés.
  - ♦ *Recommandations : chiffrer systématiquement les données sensibles (données sensibles au sens de l'article 8 et les données relevant de l'article 9 de la loi informatique et libertés) archivées.*
- Vérifier que les autorités d'archivage disposent d'une politique d'archivage (PA).
  - ♦ *Recommandations : le document de PA devrait formaliser les contraintes juridiques, fonctionnelles, opérationnelles et techniques à respecter par les différents acteurs afin que l'archivage électronique mis en place puisse être considéré comme fiable et pérenne.*
- Vérifier qu'il existe une déclaration des pratiques d'archivage (DPA).
  - ♦ *Recommandations : le document de DPA devrait décrire tous les moyens mis en œuvre pour atteindre les objectifs fixés dans la PA.*

Outillage / Pour aller plus loin

- Voir le guide ANSSI Archivage à venir et la norme NF-42-013.
- Voir le site des archives de France.

4 Chiffrement

4.1 Mesures génériques

Objectifs : rendre les données à caractère personnel incompréhensibles à toute personne non autorisée à y avoir accès (chiffrement symétrique ou asymétrique, utilisation d'algorithmes publics réputés forts, certificat d'authentification, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Déterminer ce qui doit être chiffré (un disque dur entier, une partition, un conteneur , certains fichiers, des données d'une base de données, un canal de communication, etc.) selon la forme de stockage des données, les risques identifiés et les performances exigées .
- Choisir le type de chiffrement (symétrique ou asymétrique) selon le contexte et les risques identifiés.
- Recourir à des solutions de chiffrement basées sur des algorithmes publics réputés forts.
    - ♦ *Recommandations : employer des outils (dispositifs de protection des clés privées, module de chiffrement et module de déchiffrement) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information au niveau correspondant à la robustesse attendue.*
- Mettre en place des mesures pour garantir la disponibilité, l'intégrité et la confidentialité des éléments permettant de récupérer des secrets perdus (mots de passe administrateurs, CD de recouvrement, etc.).

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Confidentialité » du référentiel général de sécurité (RGS).

4.2 Spécificités pour un chiffrement symétrique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une clé que pour un seul usage.
- Choisir un mécanisme reconnu par les organisations compétentes.
    - ♦ *Recommandations : employer des mécanismes conformes au RGS tels que l'algorithme AES , employer une taille de blocs traités au moins égale à 128 bits, un mode opératoire de chiffrement non déterministe (tel qu'un mécanisme CBC avec un vecteur d'initialisation aléatoire), des clés cryptographiques de longueur conforme à la durée d'utilisation prévue (par*

exemple, au moins 128 bits pour une confidentialité assurée jusqu'en 2020) et qui ne soient pas des clés faibles, etc.

- Formaliser la manière dont les clés vont être gérées.
  - ♦ *Recommandations : rédiger une procédure.*

4.3 Spécificités pour un chiffrement asymétrique (ou à clé publique)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une bi-clé que pour un seul usage.
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
  - ♦ *Recommandations : employer des mécanismes conformes au RGS tels que RSAES-OAEP, employer des clés cryptographiques de longueur conforme à la durée d'utilisation prévue (par exemple, au moins 128 bits pour une confidentialité assurée jusqu'en 2020).*
- Générer les clés conformément au RGS.
  - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique (PSCE) référencé conforme au RGS dans sa version 1.0 pour un usage de chiffrement.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
  - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification correcte à tous les niveaux.*
- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
  - ♦ *Recommandations : le stockage des clés des utilisateurs est protégé (règles restrictives de droits d'accès, mot de passe, carte à puce à code, etc.), la génération et l'utilisation des clés racines d'une infrastructure de gestion des clés (celles qui vont être utilisées pour signer les autres clés) font l'objet de mesures de sécurité renforcée (ex. : obligation de réunir plusieurs détenteurs d'une partie des secrets pour utiliser les clés, stockage dans un coffre-fort), etc.*
- Formaliser la manière dont les clés vont être gérées.
  - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations.*

4.4 Spécificités pour le chiffrement de matériels

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à la récupération d'un matériel (poste de travail, serveur, support amovible, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données au niveau matériel (surface du disque dur) ou au niveau du système d'exploitation (chiffrement d'une partition ou d'un conteneur).
  - ♦ *Recommandations : utiliser des équipements chiffrables tels que des disques durs avec une technologie SED , ou des logiciels tels que dm-crypt sous Linux, FileVault sous MacOS, VeraCrypt sous Windows.*
- Privilégier les dispositifs ne stockant pas les clés sur le matériel à chiffrer sauf à ce que celui ci mette en œuvre un dispositif de stockage sécurisé (par exemple une puce TPM pour les ordinateurs portables).

4.5 Spécificités pour le chiffrement de bases de données

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés au vol du serveur, à un accès physique illégitime au poste de travail ou au serveur et à un accès direct aux données du serveur par un administrateur .

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Selon les risques identifiés, chiffrer l'espace de stockage (au niveau matériel, du système d'exploitation ou de la base de données) afin de se protéger d'un vol physique, de la donnée elle-même (chiffrement par l'application) afin de garantir la confidentialité de certaines données vis à vis des administrateurs eux-mêmes. Le chiffrement par la base de données peut dans le cas d'équipes informatiques cloisonnées permettre de rendre les données uniquement accessibles des administrateurs de base de données sans que les administrateurs système y aient accès.

4.6 Spécificités pour le chiffrement de partitions ou de conteneurs

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à la récupération d'un matériel (poste de travail, serveur, support amovible, etc.), un accès physique illégitime à un poste de travail ou au serveur et un accès direct aux données du serveur par un administrateur.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données au niveau du système d'exploitation (chiffrement d'une partition, d'un répertoire ou d'un fichier) ou à l'aide d'un logiciel spécialisé (chiffrement d'un conteneur).
  - ♦ *Recommandations : utiliser des logiciels tels que VeraCrypt ou Zed!.*

4.7 Spécificités pour le chiffrement de fichiers isolés

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés au vol d'un poste de travail ou du serveur, un accès physique illégitime à un poste de travail ou au serveur et un accès direct aux données du serveur par un administrateur.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les fichiers stockés ou les pièces à joindre à des courriers électroniques.
  - ♦ *Recommandations : utiliser des logiciels tels que ZoneCentral, ceux utilisant la librairie Security BOX Crypto 6.0, ou encore AxCrypt ou Gnu Privacy Guard (GPG). A défaut, utiliser au moins un outil de compression qui permet de chiffrer avec mot de passe, tel que 7-Zip qui permet le chiffrement AES, ou bien recourir à une solution matérielle telle qu'une carte Bull Trustway PCI cryptographic card, etc.*

4.8 Spécificités pour le chiffrement de courriers électroniques

Objectifs : rendre les données contenues dans des courriers électroniques inintelligibles à toute personne non autorisée pour réduire les risques liés à l'interception de messages électroniques.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les messages électroniques.
  - ♦ *Recommandations : utiliser des logiciels tels que Gnu Privacy Guard (GPG).*

4.9 Spécificités pour le chiffrement d'un canal de communication

Objectifs : rendre les données inintelligibles à toute personne non autorisée à y avoir accès pour réduire les risques liés à l'interception de flux de données.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer le canal de communication entre un serveur authentifié et un client distant.
  - ♦ *Recommandations : utiliser un certificat d'authentification de serveur conforme au RGS et le protocole TLS (anciennement SSL) dans ces dernières versions (penser à exiger d'entrer un mot de passe pour utiliser la clé privée et à protéger l'accès à celle-ci par des droits d'accès très restrictifs), ou bien SSH pour mettre en place un tunnel sécurisé (VPN), ou encore des solutions de chiffrement IP (VPN-IPSec), etc.*

5 Cloisonnement des données (par rapport au reste du système d'information)

Objectifs : réduire la possibilité de corréler des données à caractère personnel et de provoquer une violation de l'ensemble des données (identifier les données propres à chaque métier, les séparer logiquement, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier les seules données utiles à chaque processus métier.
  - ♦ *Recommandations : prévoir un accès des personnes aux seules données dont elles ont besoin. Par exemple, le service statistiques n'a pas accès aux noms et prénoms.*
- Séparer logiquement les données utiles à chaque processus.
  - ♦ *Recommandations : gérer des droits d'accès différenciés selon les processus métiers (gestion de la paie, gestion des congés, gestion de l'avancement de carrière, etc.), disposer d'un environnement informatique dédié pour les systèmes traitant des données les plus sensibles, etc.*
- Vérifier de manière régulière que les données sont bien cloisonnées, et que des destinataires ou des interconnexions n'ont pas été ajoutés.

6 Contrôle d'accès physique

Objectifs : limiter les risques que des personnes non autorisées n'accèdent physiquement aux données à caractère personnel (liste des personnes autorisées, authentification des collaborateurs et des visisteurs, trace des accès, alerte en cas d'effraction, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Distinguer les zones des bâtiments selon les risques.
  - ♦ *Recommandations : délimiter une zone ouverte au public lorsqu'il y a une obligation fonctionnelle d'accueil (comptoir d'accueil, salle d'attente ou de réunion, etc.), une zone réservée au service (zone à accès contrôlé correspondant aux bureaux où sont traitées les données), et une zone de sécurité (elle héberge les serveurs, les stations d'administration du réseau, les éléments actifs du réseau ou certaines ressources sensibles telles que des équipements d'alimentation et de distribution d'énergie, ou des équipements réseau et de téléphonie).*
- Tenir à jour une liste des personnes (visiteurs, employés, employés habilités, stagiaires, prestataires, etc.) autorisées à pénétrer dans chaque zone.
  - ♦ *Recommandations : réexaminer régulièrement les droits d'accès aux zones de sécurité, les supprimer si nécessaire.*
- Choisir des moyens d'authentification des collaborateurs proportionnels aux risques selon chaque zone.
  - ♦ *Recommandations : si les risques ne sont pas élevés, une personne à l'accueil peut suffire pour reconnaître les collaborateurs, alors que s'ils sont plus élevés (zone réservée ou de sécurité), l'usage d'un portillon ou d'un autre moyen de contrôle d'accès avec un badge de proximité comportant la photographie d'identité du porteur et/ou un numéro d'identification personnel est conseillé, le badge devant être porté de manière visible.*
- Choisir des moyens d'authentification des visiteurs (personnes venant en réunion, prestataires externes, auditeurs, etc.) proportionnels aux risques selon chaque zone.
  - ♦ *Recommandations : si les risques ne sont pas élevés, l'authentification peut ne pas être nécessaire ; en revanche, si les risques sont élevés, il convient de mettre en place un accueil des visiteurs externes dans une grille horaire prédéfinie, de vérifier leur pièce d'identité, puis de leur fournir un badge spécifique qui ne fonctionnera que pendant la durée de leur visite.*
- Déterminer les actions à entreprendre en cas d'échec de l'authentification (impossible de vérifier une identité, défaut d'habilitation à pénétrer dans une zone sécurisée, etc.).
  - ♦ *Recommandations : refuser l'accès au visiteur, prévenir la personne en charge de la sécurité, etc.*
- Conserver une trace des accès après en avoir informé les personnes concernées.

- ♦ *Recommandations : enregistrer l'identité, la date et l'heure de l'entrée, ainsi que la date et l'heure de la sortie des visiteurs, tenir à jour un journal des accès des trois derniers mois au plus.*

- Faire accompagner les visiteurs, en dehors des zones d'accueil du public (depuis leur entrée, pendant leur visite et jusqu'à leur sortie des locaux) par une personne appartenant à l'organisme.
- Protéger les zones les plus sensibles de manière proportionnelle aux risques.
  - ♦ *Recommandations : mettre en place une porte verrouillée, un digicode ou un vidéophone, renouveler régulièrement les moyens d'accès (code des digicodes), identifier la zone avec une signalétique claire, visible et compréhensible par tout public, sécuriser les ouvrants (barreaux aux fenêtres pour les locaux situés au rez-de-chaussée ou bas étages, porte renforcée avec digicode).*
- Installer un dispositif permettant d'être alerté en cas d'effraction.
  - ♦ *Recommandations : équiper les ouvrants de systèmes de détection des ouvertures et de détection d'effraction faisant remonter les alertes de manière centralisée (gardiennage local, prestations externalisées, etc.) notamment dans les zones de sécurité, surveiller les zones les plus sensibles à l'aide d'un dispositif de vidéosurveillance.*

Outillage / Pour aller plus loin

- Prévoir les moyens de ralentir les personnes qui auraient pénétré dans une zone dont l'accès leur est interdit, ainsi que les moyens d'intervention dans de telles situations, de telle sorte que le délai d'intervention soit inférieur au temps qu'il faut aux personnes non autorisées pour sortir de la zone.

7 Contrôle d'intégrité

7.1 Mesures génériques

Objectifs : être alerté en cas de modification non désirée ou de disparition de données à caractère personnel (fonction de hachage, code d'authentification de message, signature électronique, prévenir les injections SQL, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier les données dont l'intégrité doit être contrôlée selon les risques identifiés.
- Choisir un moyen de contrôler l'intégrité selon le contexte, les risques appréciés et la robustesse attendue.
    - ♦ *Recommandations : utiliser une fonction de hachage pour générer une empreinte (hash) des données afin de traiter les risques liés aux erreurs, appliquer un code d'authentification de messages (MAC) afin de traiter les risques liés aux erreurs et à la modification par toute personne ignorant la clé, appliquer une fonction de signature électronique afin de traiter les risques liés aux erreurs et à la modification par toute personne autre que le signataire, etc.*
- Définir le moment auquel la fonction est appliquée et celui où le contrôle doit être effectué selon le déroulement du processus métier.
    - ♦ *Recommandations : si l'on veut contrôler l'intégrité de données à chaque utilisation, une empreinte de chaque donnée peut être réalisée à la saisie, une autre empreinte peut être réalisée à chaque affichage, et une alerte visuelle peut apparaître si elles ne correspondent pas (auquel cas on pourra restaurer les données si elles ont été préalablement sauvegardées), etc.*
- Lorsque les données sont envoyées dans une base de données, il est nécessaire de mettre en place des mesures d'analyse permettant de prévenir les attaques par injection SQL ou de scripts.
    - ♦ *Recommandations : empêcher la saisie de n'importe quelle donnée (caractère spéciaux, commandes SQL, etc.), filtrer ou encoder les données avant leur enregistrement, limiter le volume des données pouvant être saisi.*

7.2 Spécificités pour une fonction de hachage

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser un mécanisme reconnu par les organisations compétentes.
    - ♦ *Recommandations : utiliser une fonction de hachage conforme au référentiel général de sécurité (RGS) telle que SHA-256 pour calculer une empreinte sur les données et la transmettre (par un canal différent ou après l'avoir signée électroniquement) afin que l'intégrité des données soit vérifiée au moment de*

leur réception dans le cas d'un envoi par courrier électronique, ou bien la stocker de manière sécurisée afin que le contrôle d'intégrité puisse être réalisé lors de leur utilisation dans le cas de sauvegardes, d'archivage ou simplement de stockage, etc.

7.3 Spécificités pour un code d'authentification de message

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

• Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.

♦ *Recommandations : utiliser un algorithme de calcul de code d'authentification de message conforme au RGS tel que le CBC-MAC « retail » utilisant l'AES comme mécanisme de chiffrement par bloc et deux clés distinctes (une pour la chaîne CBC et l'autre pour le surchiffrement dit « retail »).*

7.4 Spécificités pour une fonction de signature électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une bi-clé que pour un seul usage.
- Recourir à des solutions de signature basées sur des algorithmes publics réputés forts.
  - ♦ *Recommandations : employer des outils (dispositifs de création de signature, application de création de signature et module de vérification de signature) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information (ANSSI), au niveau correspondant à la robustesse attendue.*
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
  - ♦ *Recommandations : employer des mécanismes conforme au RGS tels que RSA-SSA-PSS, ou bien ECDSA en utilisant l'une des courbes P-256, P-384, P-521, B-283, B-409 ou B-571, etc.*
- Générer les clés conformément au RGS.
  - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 2 pour un usage de signature.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
  - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification qui est correcte à tous les niveaux.*

- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
- Formaliser la manière dont les clés vont être gérées.
    - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations, etc.*

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Signature électronique » du RGS.

Notes

- Dans le cas de l'utilisation d'une carte à puce comme dispositif de création de signature, il est recommandé d'utiliser un lecteur de carte à puce avec PIN-pad intégré permettant de saisir son code d'activation et de le vérifier sans que celui-ci ne transite via l'ordinateur ou la borne d'accès publique utilisés.

8 Contrôle des accès logiques

Objectifs : limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel par voie électronique (gestion de profils utilisateurs, mécanisme d'authentification, politique de mots de passe, etc.).

8.1 Gérer les privilèges des utilisateurs sur les données

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Gérer les profils d'utilisateurs en séparant les tâches et les domaines de responsabilité, de préférence de manière centralisée, afin de limiter l'accès aux données aux seuls utilisateurs habilités, en appliquant les principes du besoin d'en connaître et du moindre privilège.
    - ♦ *Recommandations : définir un ou plusieurs profils d'utilisateurs de façon centralisée (avec des privilèges spécifiques d'utilisation des fonctionnalités, de création, d'accès, de modification, de transfert et de suppression des données), faire rattacher chaque personne à un des profils définis en début de contrat ou de changement d'emploi.*
- Identifier toute personne ayant un accès légitime aux données (employés, contractants et autres tiers) par un identifiant unique.
- Dans le cas où l'utilisation d'identifiants génériques ou partagés est incontournable, obtenir une validation de la hiérarchie et mettre en œuvre des moyens de traçabilité de l'utilisation de ce type d'identifiant.
    - ♦ *Recommandations : renseigner une fiche de présence, remplir une main courante des actions, etc.*
- Limiter l'accès aux outils et interfaces d'administration aux personnes habilitées.
- Limiter l'utilisation des comptes permettant de disposer de privilèges élevés aux opérations qui le nécessitent.
- Limiter l'utilisation des comptes « administrateurs » au service en charge de l'informatique et ce, uniquement pour les actions d'administration qui le nécessitent.
    - ♦ *Recommandations : les comptes « administrateurs » ne doivent être réservés qu'aux tâches d'administrations ; les administrateurs doivent utiliser un compte ayant des droits plus limités lorsqu'ils effectuent des actions plus exposées (ex : lecture de mail, internet, etc.).*
- Chaque compte, et d'autant plus s'il a des privilèges élevés (ex : compte administrateur), doit avoir un mot de passe propre.
    - ♦ *Recommandations : les comptes « administrateurs » doivent être, autant que possible, individuels et requérir un mot de passe personnel.*
- Journaliser les informations liées à l'utilisation des privilèges (voir la page Traçabilité (journalisation)).
- Réaliser une revue annuelle des privilèges afin d'identifier et de supprimer les comptes non utilisés, et de réaligner les privilèges sur les fonctions de chaque utilisateur.

- Retirer les droits des employés, contractants et autres tiers dès lors qu'ils ne sont plus habilités à accéder à un local ou à une ressource ou à la fin de leur contrat, et les ajuster en cas de changement de poste. Pour les personnes ayant un compte temporaire
(stagiaire, prestataire...), configurer une date d'expiration à la création du compte.

8.2 Authentifier les personnes désirant accéder aux données

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Choisir un moyen d'authentification pour les ouvertures de session, adapté au contexte, au niveau des risques et à la robustesse attendue.
    - ♦ *Recommandations : si les risques ne sont pas élevés, l'usage d'un mot de passe est envisageable ; en revanche, si les risques sont plus élevés, il convient d'utiliser un boitier électronique générateur de mots de passe à usage unique OTP (token), sans oublier de changer les mots de passe d'activation par défaut, ou sur l'envoi d'une partie du mot de passe par SMS, une carte avec code PIN, un certificat électronique ou tout autre moyen d'authentification forte.*
- Interdire que les mots de passe utilisés apparaissent en clair dans les programmes, fichiers, scripts, traces ou fichiers journaux, ou à l'écran lors de leur saisie.
- Déterminer les actions à entreprendre en cas d'échec de l'authentification.
    - ♦ *Recommandations : bloquer le compte après cinq échecs de connexion, accroître le temps d'attente entre deux tentatives de connexion?*
    - ♦ *Journaliser les informations liées aux accès logiques (voir la page Traçabilité (journalisation)).*
- Limiter l'authentification par identifiants et mots de passe au contrôle de l'accès au poste de travail (déverrouillage uniquement).
- Authentifier le poste de travail auprès du système d'information distant (serveurs) à l'aide de mécanismes cryptographiques.

Notes

- Un mécanisme d'authentification forte requiert au minimum deux facteurs d'authentification distincts parmi ce que l'on sait (ex. : mot de passe), ce que l'on a (ex. : certificat électronique, carte à puce, etc.) et une caractéristique qui nous est propre (ex. : empreinte digitale ou autre caractéristique biométrique).
- Dans un environnement informatique peu sécurisé (ex. : postes partagés), prévoir une deuxième authentification pour l'accès à l'application contenant des données.
- La loi informatique et libertés subordonne le recours à des dispositifs biométriques à l'autorisation préalable de la CNIL. D'une manière générale, la CNIL recommande l'utilisation de biométrie sans traces (contour de la main, réseaux veineux, etc.) ou l'enregistrement des empreintes digitales dans un support individuel.

Outillage / Pour aller plus loin

- Voir les exigences relatives à la fonction « Authentification » du référentiel général de sécurité (RGS).
- Voir le document CNIL Empreinte sur les dispositifs basés sur l'empreinte digitale.
- Des solutions de contrôle d'accès au réseau (NAC ? *Network Access Control*) sont préconisées dès lors qu'un nombre important d'utilisateurs doit être géré.

8.3 Spécificités pour une authentification par certificat électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'employer une clé que pour un seul usage .
- Recourir à des solutions d'authentification basées sur des algorithmes publics réputés forts.
    - ♦ *Recommandations : employer des outils (dispositif d'authentification, application d'authentification et module de vérification d'authentification) certifiés, qualifiés ou faisant l'objet d'une certification de sécurité de premier niveau par l'agence nationale de la sécurité des systèmes d'information, au niveau correspondant à la robustesse attendue.*
- Choisir un mécanisme reconnu par les organisations compétentes et qui dispose d'une preuve de sécurité.
    - ♦ *Recommandations : employer des mécanismes conforme au RGS tels que RSA-SSA-PSS, ou bien ECDSA en utilisant l'une des courbes P-256, P-384, P521, B-283, B-409 ou B-571*
- Générer les clés conformément au RGS.
    - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 1.0 pour un usage d'authentification.*
- Mettre en place des mécanismes de vérification des certificats électroniques.
    - ♦ *Recommandations : lors de la réception d'un certificat électronique, vérifier au minimum que le certificat contient une indication d'usage conforme à ce qui est attendu, qu'il est valide et non révoqué, et qu'il a une chaîne de certification qui est correcte à tous les niveaux.*
- Protéger la sécurité de la génération et de l'utilisation des clés en cohérence avec leur niveau dans la hiérarchie des clés.
- Formaliser la manière dont les clés vont être gérées.
    - ♦ *Recommandations : élaborer une « politique de certification » qui précise les responsabilités, l'identification et l'authentification, les exigences opérationnelles dans le cycle de vie des certificats, les mesures de sécurité non techniques et techniques, les profils des certificats et listes de révocation, les audits de conformité et autres évaluations?.*

8.4 Gérer les authentifiants

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Adopter une politique de mots de passe, la mettre en œuvre et la contrôler automatiquement dans la mesure où les applications et les ressources le permettent, et y sensibiliser les utilisateurs.
    - ♦ *Recommandations : les mots de passe sont constitués de huit caractères minimum, ils doivent être renouvelés au moindre doute de compromission et éventuellement de manière périodique (tous les six mois ou une fois par an), ils comprennent au minimum trois types de caractères parmi les quatre types de caractères (majuscules, minuscules, chiffres et caractères spéciaux) ; lors d'un changement de mot de passe, il est interdit de réutiliser un des cinq derniers mots de passe ; éviter d'utiliser le même mot de passe pour des accès différents ; éviter de choisir des mots de passe ayant un lien avec soi (nom, date de naissance?)?*
- Adopter une politique spécifique de mots de passe pour les administrateurs, la mettre en œuvre et la contrôler automatiquement dans la mesure où les applications et les ressources le permettent, et y sensibiliser les administrateurs.
    - ♦ *Recommandations : les mots de passe doivent respecter la Délibération n° 2017-012 du 19 janvier 2017. En outre, il convient de ne jamais utiliser le même mot de passe pour des accès différents, d'éviter de choisir des mots de passe ayant un lien avec soi (nom, date de naissance?), de configurer les logiciels pour qu'ils ne retiennent jamais les mots de passe, de définir un nombre de tentatives maximum au-delà duquel une alerte est émise et l'authentification est bloquée (temporairement ou jusqu'à ce qu'elle soit manuellement débloquée).*
- Modifier immédiatement après installation d'une application ou d'un système les mots de passe par défaut.
- Créer chaque compte utilisateur avec un mot de passe initial aléatoire unique, le transmettre de manière sécurisée à l'utilisateur, par exemple en utilisant deux canaux séparés (papier et autres) ou une « case à gratter », et le contraindre à le modifier lors de sa première connexion et lorsque qu'un nouveau mot de passe lui est fourni (par exemple en cas d'oubli).
- Stocker les informations d'authentification (mots de passe d'accès aux systèmes d'information, clés privés liées aux certificats électroniques?) de façon à être accessibles uniquement par des utilisateurs autorisés.
    - ♦ *Recommandations : limiter les droits d'accès (lecture, écriture, etc.) au strict minimum, chiffrer les fichiers dans lesquels on note ses mots de passe.* Placer les authentifiants permettant l'administration des ressources des systèmes informatiques sous séquestre et les tenir à jour, dans un coffre ou une armoire fermé à clé.
- Dans le cas où de nombreux mots de passe ou secrets (clés privées, certificats, etc.) doivent être utilisés, mettre en place une solution d'authentification centralisée, de mots de passe à usage unique ou de coffres-forts sécurisés.

- *Recommandations : contrôle d'accès constitué au minimum par un mot de passe maître robuste, stockage sécurisé des mots de passe garantissant que les mots de passe protégés ne peuvent être récupérés sans connaissance du secret (chiffrement, masquage, etc.), affichage sécurisé des mots de passe (masquage des mots de passe dans les boîtes de connexion, etc.), résistance aux attaques (déchiffrement, force brute, rejeu, etc.), fermeture ou blocage automatique (après une certaine durée, lors de la mise en veille sécurisée, etc.).*
- En cas de départ d'un administrateur disposant de privilèges sur des composants des systèmes informatiques, désactiver les comptes individuels dont il disposait et changer les éventuels mots de passe d'administration dont il avait connaissance (mots de passe des comptes fonctionnels, comptes génériques ou comptes de service utilisés dans le cadre des fonctions de l'administrateur, etc.).

Notes

- Des moyens mnémotechniques permettent de créer des mots de passe complexes, par exemple :
  - en ne conservant que les premières lettres des mots d'une phrase ;
  - en mettant une majuscule si le mot est un nom (ex : Chef) ;
  - en gardant des signes de ponctuation (ex : ') ;
  - en exprimant les nombres à l'aide des chiffres de 0 à 9 (ex : Un ->1).
- *Ainsi, la phrase « un Chef d'Entreprise averti en vaut deux » correspond au mot de passe 1Cd'Eaev2.*
- Il convient d'être vigilant à supprimer toute donnée d'authentification à caractère biométrique intervenant dans des dispositifs de contrôle d'accès.

Outillage / Pour aller plus loin

- Voir la note CERTA MotsDePasse.

9 Durées de conservation : limitées

Objectifs : être conforme aux articles 6 et 36 de la loi informatique et libertés et l'article 5.1(e) du règlement général sur la protection des données (RGPD) ; réduire la gravité des risques en s'assurant que les données à caractère personnel ne seront pas conservées plus que nécessaire.

Bonnes pratiques

- Définir, pour chaque catégorie de données, des durées de conservation limitées dans le temps et en adéquation avec la finalité du traitement et/ou des contraintes légales.
  - ♦ *Recommandations : définir des durées de conservation adaptées à chaque type de données traitées ; distinguer les données courantes, les données archivées (dont l'accès sera restreint aux seuls acteurs concernés), les traces fonctionnelles, les journaux techniques (logs).*
- Vérifier que le traitement permet de détecter la fin de la durée de conservation (mettre en place un mécanisme automatique basé sur la date de création des données ou de leur dernier usage).
  - ♦ *Recommandations : le traitement affiche la date a laquelle la donnée va ou doit être supprimée.*
- Vérifier que le traitement permet de supprimer les données en fin de durée de conservation et que le moyen choisi pour les supprimer est approprié aux risques qui pèsent sur les libertés et la vie privée des personnes concernées.
  - ♦ *Recommandations :* La suppression d'une donnée arrivée au terme de sa durée de conservation ne peut être logique (indicateur d'état indiquant que la donnée est effacée mais permettant toujours de la lire directement dans la base de données).
  - ♦ Une bonne pratique peut consister à définir une durée de conservation intermédiaire permettant de ne rendre les données accessible de tous que pendant une certaine période puis passé un certain délai uniquement par une liste restreinte de personne (Ex. la donnée reste accessible de tous pendant 6 mois puis uniquement par le service contentieux ensuite).
- Une fois la durée de conservation atteinte, sous réserve de l'archivage intermédiaire pour les données qui le nécessitent, supprimer les données sans délai (voir également la page Minimisation des données : adéquates, pertinentes et limitées).
  - ♦ *Recommandations : développer une fonctionnalité automatisée qui archive/efface les données dont la durée de conservation est atteinte, y compris pour les traces et journaux techniques. Dans le cas ou l'effacement est effectué manuellement, l'outil doit mettre à disposition de l'utilisateur une fonctionnalité d'effacement par lot.*
  - ♦ *Le cas échéant, lorsque le contexte le permet, la durée de conservation d'une donnée peut être prolongée par l'utilisateur. Par défaut, la donnée est effacée au terme initialement prévu.*

Notes

- D'une manière générale, la finalité des traitements ne justifie pas de conserver des données en prévisions d'actions de Police ou en Justice au-delà de ce qui est prévu conformément à la loi informatique et libertés et au RGPD. Toutefois, dans certains secteurs, il est obligatoire de conserver certaines données pendant une durée déterminée (opérateurs de télécommunication, passagers de vols aériens, etc.).
- En réduisant la quantité de données traitées et disponibles, l'archivage et la purge permettent de limiter les impacts en cas de vol ou de diffusion accidentelle de la base de données.

10 Eloignement des sources de risques

Objectifs : éviter que des sources de risques, humaines ou non humaines, portent atteinte aux données à caractère personnel (produits dangereux, zones géographiques dangereuses, transfert des données en dehors de l'UE, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Placer les produits dangereux (inflammables, combustibles, corrosifs, explosifs, aérosols, humides, etc.) dans des lieux de stockage appropriés et éloignés de ceux où sont traitées des données.
- Éviter les zones géographiques dangereuses (zones inondables, proximité d'aéroports, zones d'industries chimiques, zones sismiques, zones volcaniques, etc.).
- Ne pas stocker les données dans un état étranger sauf s'il existe des garanties permettant d'assurer un niveau de protection des données suffisant : si le transfert a lieu vers un pays reconnu comme "adéquat" par la Commission européenne - Canada, Suisse, Argentine, territoires de Guernesey, Jersey et Isle de Man ? ou si des clauses contractuelles types, approuvées par la Commission européenne, sont signées entre deux entreprises ou si des règles internes d'entreprises (*Binding Corporate Rules* - BCR) sont adoptées au sein d'un groupe ou si dans le cas d'un transfert vers les États-Unis, l'entreprise destinataire a adhéré au *Privacy Shield* ou si l'une des exceptions prévues par l'article 69 de la loi Informatique et libertés est invoquée. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des données stockées et doit s'assurer du niveau de sécurité du stockage.

11 Exercice des droits de limitation du traitement et d'opposition

11.1 Mesures génériques

Objectifs : être conforme à l'article 38 de la loi informatique et libertés et les articles 18 et 21 du règlement général sur la protection des données (RGPD) : garantir aux personnes la possibilité de s'opposer à l'utilisation de données à caractère personnel qui les concernent ; permettre à l'utilisateur d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité, par exemple ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 38 de la loi informatique et libertés (obligation légale, exclusion dans l'acte portant création du traitement) et à l'article 21 du RGPD (motifs légitimes et impérieux, droits en justice, intérêt public) interdisant à la personne de s'opposer au traitement.

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'opposition. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.
- S'assurer que le droit d'opposition pourra toujours s'exercer et que les données collectées et traitées permettent effectivement l'exercice du droit d'opposition.
    - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que « l'intéressé est mis en mesure d'exprimer son choix avant la validation définitive de ses réponses », conformément à l'article 96 du décret informatique et libertés.
    - ♦ *Recommandations : vérifier que le droit d'opposition peut s'exercer avant la validation définitive des réponses des personnes concernées ou avant la fin de la collecte.*
- Vérifier que les demandes d'exercice du droit d'opposition faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater.
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse.
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).

- S'assurer que le motif légitime des personnes exerçant leur droit d'opposition est fourni et apprécié (sauf dans le cas de la prospection et des traitements ayant pour fin la recherche dans le domaine de la santé relevant du chapitre IX de la loi informatique et libertés, pour lesquels la personne dispose d'un droit d'opposition discrétionnaire).
- S'assurer que tous les destinataires du traitement seront informés des oppositions exercées par des personnes concernées, conformément à l'article 97 du décret informatique et libertés.

Notes

- Le droit à la limitation permet à la personne concernée d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité, par exemple.

11.2 Spécificités pour un traitement par téléphone

Bonnes pratiques

• Prévoir un mécanisme permettant aux personnes concernées de signifier leur opposition à l'aide du téléphone.

♦ *Recommandations : prévoir la possibilité de s'opposer en appuyant sur une touche.*

11.3 Spécificités pour un traitement par formulaire électronique

Bonnes pratiques

• Créer un formulaire, facilement accessible, avec des cases à décocher (dit « *opt-out* ») ou prévoir la possibilité de se désinscrire d'un service (suppression de compte).

11.4 Spécificités pour un traitement par courrier électronique

Bonnes pratiques

- S'assurer que l'expéditeur des messages apparaît très clairement.
- S'assurer que le corps des messages est en rapport avec le sujet des messages.
- Prévoir une opposition en répondant au message ou en cliquant sur un lien permettant de s'opposer. La personne ne doit pas avoir besoin de s'authentifier pour être désinscrite.

11.5 Spécificités pour un traitement par un objet connecté ou une application mobile

Bonnes pratiques

- Proposer des paramètres « Vie privée ».
  - ♦ *Recommandations : inviter l'utilisateur à changer les paramètres par défaut ; rendre ces paramètres accessibles au premier démarrage de l'appareil ou de l'application, et ensuite à tout moment par un menu spécifique.*
- Permettre à l'utilisateur de s'opposer à la collecte de données particulières.
  - ♦ *Recommandations : prévenir l'utilisateur (icône, voyant lumineux) quand l'application fonctionne en arrière plan, quand l'appareil "écoute" avec le micro, quand la localisation est collectée, etc. et lui permettre de s'y opposer.*
- Prendre en compte les utilisateurs mineurs.
  - ♦ *Recommandations : proposer un dispositif de contrôle parental, exclure les enfants de moins de 13 ans de tout traitement de profilage automatisé.*
- Arrêter effectivement toute collecte de données si l'utilisateur retire son consentement.

11.6 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN)

Bonnes pratiques

- Si les prélèvements sont conservés pour un traitement ultérieur différent du traitement initial, permettre également aux personnes concernées par cet autre traitement de s'y opposer et ce, sans requérir un motif légitime.

12 Exercice des droits de rectification et d'effacement

12.1 Mesures génériques

Objectifs : être conforme à l'article 40 de la loi informatique et libertés et les articles 16, 17 et 19 du règlement général sur la protection des données (RGPD) ; garantir aux personnes la possibilité de rectifier, compléter, mettre à jour, verrouiller ou supprimer des données à caractère personnel qui les concernent ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée à l'article 41 de la loi informatique et libertés (sûreté de l'État, défense ou sécurité publique) ou à l'article 17 du RGPD (liberté d'expression et d'information, obligation légale, intérêt public ou d'autorité publique, santé publique, recherche scientifique ou historique ou à des fins statistiques, droits en justice).

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit de rectification. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.
- S'assurer que le droit de rectification pourra toujours s'exercer.
  - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que le droit d'effacement pourra toujours s'exercer.
  - ♦ *Recommandations : fournir des indications claires et des étapes simples pour effacer les données en cas de vente de l'appareil ou avant de le mettre au rebut ; permettre d'effacer les données à distance en cas de vol de l'appareil.*
- S'assurer que l'identité des demandeurs va être vérifiée.
  - ♦ *Recommandations : vérifier que les demandes d'exercice du droit de rectification faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve), que celles faites par voie électronique (en utilisant un canal chiffré si la transmission est faite via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conserver une preuve, et ce, en noir et blanc, en faible définition et chiffré), et qu'elles précisent l'adresse à laquelle doit parvenir la réponse, vérifier l'identité des demandeurs venant sur place et des personnes qu'ils peuvent mandater ou des héritiers d'une personne décédée, etc.*
- S'assurer que la véracité des rectifications demandées sera vérifiée.
- S'assurer de l'effacement effectif des données à supprimer.
- S'assurer qu'une confirmation sera fournie aux demandeurs.
- S'assurer que les destinataires à qui des données auraient été transmises seront informés des rectifications faites.

- Suite à une demande d'effacement, préciser à l'utilisateur si des données personnelles seront conservées malgré tout (contraintes techniques, obligations légales, etc.)
- Mettre en œuvre le droit à l'oubli pour les mineurs.
    - ♦ *Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement et sans autre motif demander au site l'effacement, dans les meilleurs délais, des données le concernant. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.*

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 99 à 100 du décret informatique et libertés.

Notes

- Le responsable de traitement dispose d'un délai d'un mois pour effacer les données ou répondre à la personne. Passé ce délai, la personne concernée peut saisir la CNIL. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.
- Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement et sans autre motif demander au site l'effacement, dans les meilleurs délais, des données le concernant.

12.2 Spécificités pour la publicité ciblée en ligne

Bonnes pratiques

• Prévoir un accès par la personne aux centres d'intérêt établis pour son profil et la possibilité de les modifier. L'authentification de la personne peut se faire sur la base des informations utilisées pour accéder à son compte ou sur la base du cookie (ou équivalent) présent sur son poste.

13 Exercice des droits d'accès et à la portabilité

13.1 Mesures génériques

Objectifs : être conforme à l'article 39 de la loi informatique et libertés et les articles 15 et 20 du règlement général sur la protection des données (RGPD) ; garantir aux personnes la possibilité de prendre connaissance des données à caractère personnel qui les concernent ; permettre à l'utilisateur de récupérer, sous une forme aisément réutilisable, les données personnelles qu'il a fournies au traitement afin de les transférer vers un autre service ; vérifier que le traitement ne fait pas l'objet d'une exception mentionnée dans les articles 39 et 41 de la loi informatique et libertés (comme des données traitées pour une finalité de statistiques ou de recherche lorsqu'il n'y a aucun risque d'atteinte à la vie privée des personnes et que les données ne sont conservées seulement le temps nécessaire à ces finalités, pour la sûreté de l'État, la défense ou la sécurité publique) et à l'article 20 du RGPD (pas de portabilité pour les traitements d'intérêt public ou d'autorités publiques, respects des droits et libertés de tiers).

Bonnes pratiques

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'accès. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois (un mois dans le cadre du RGPD) pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction.
    - ♦ *Recommandations : mettre en place un processus permettant de tenir informés les demandeurs de la prise en compte de leur demande et du traitement nécessaire (par exemple par un courrier postal ou électronique indiquant la prise en compte de la demande et le délai à prévoir pour la réponse). Dans le cas de données archivées, il existe une tolérance au niveau des délais si le responsable de traitement a informé le demandeur de ses difficultés et indiqué un délai de réponse raisonnable.*
- S'assurer que le droit d'accès pourra toujours s'exercer.
    - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- Vérifier que les demandes d'exercice du droit d'accès faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater.
- Vérifier que les demandes d'exercice du droit d'accès faites par voie postale sont signées
  et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse.
- Vérifier que les demandes d'exercice du droit d'accès faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).

- S'assurer de la possibilité de fournir toutes les informations qui peuvent être demandées par les personnes concernées, tout en protégeant les données des tiers.

Outillage / Pour aller plus loin

- Voir les articles 92 à 95 et 98 du décret informatique et libertés.
- Voir le guide CNIL-Employeurs.

13.2 Spécificités pour l'accès aux dossiers médicaux

Bonnes pratiques

- Communiquer les informations au plus tard dans les huit jours suivant la demande et dans les deux mois si les informations remontent à plus de cinq ans (à compter de la date à laquelle l'information médicale a été constituée).
- Permettre l'exercice du droit d'accès par les titulaires de l'autorité parentale, pour les mineurs, ou le représentant légal, pour les personnes faisant l'objet d'une mesure de tutelle, conformément à l'article 58 de la loi informatique et libertés.

Outillage / Pour aller plus loin

- Voir le décret-2002-637.

14 Finalités : déterminées, explicites et légitimes

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et à l'article 5.1(b) du règlement général sur la protection des données (RGPD) ; éviter les usages incompatibles et le détournement de finalité.

Bonnes pratiques

- Détailler les finalités de traitement des données et justifier leur légitimité.
- Expliciter les finalités de partage avec des tiers ainsi que les finalités de traitement de données pour l'amélioration du service.
- Expliciter les modalités particulières du traitement, en précisant notamment les croisements de données s'il y a lieu.

15 Fondement : licéité du traitement, interdiction du détournement de finalité

Objectifs : être conforme à l'article 6 du règlement général sur la protection des données (RGPD).

Bonnes pratiques

• Déterminer et justifier le critère de licéité qui s'applique au traitement de données considéré :

- ♦ la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- ♦ le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci
- ♦ le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- ♦ le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- ♦ le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- ♦ le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Notes

- Dans le cas d'une obligation légale ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, préciser dans la justification le fondement légal du traitement dans le droit de l'Union européenne ou de l'État membre auquel le responsable du traitement est soumis.
- Il peut y avoir plusieurs fondements pour un traitement : par exemple, un contrat lié à l'achat du produit pour son utilisation dans sa finalité principale et un consentement pour ses finalités secondaires (amélioration du service, marketing?) qui sera recueilli lors de l'activation du produit.
- Attention : si les données sont traitées à une fin autre que celle pour laquelle elles ont été collectées et que le traitement n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union européenne ou d'un État membre, il est nécessaire de déterminer si cette autre fin est compatible avec la finalité initiale de collecte, en tenant compte, entre autres :

- de l'existence éventuelle d'un lien entre la finalité du traitement et la finalité initiale de collecte des données ;
- du contexte de collecte initiale, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données ou des données relatives à des condamnations pénales et à des infractions ;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

16 Formalités préalables

Objectifs : respecter les obligations en matière de formalités préalables au traitement des données.

Bonnes pratiques

- Déclarer le traitement auprès de la CNIL préalablement à la mise en œuvre du traitement.
- Vérifier que le traitement de données est effectivement conforme à la finalité déclarée.
- Réaliser une étude d'impact sur la vie privée (EIVP ou PIA) et le faire valider.
- Consulter la CNIL si les risques résiduels sont importants, selon l'article 36 du règlement général sur la protection des données (RGPD).
- Réaliser les autres formalités sectorielles et contractuelles applicables au traitement (par exemple, formalités liées à d'autres codes et règlements, contrat avec une source externe de données, etc.)

Outillage / Pour aller plus loin

- Voir la méthode PIA et les guides PIA de la CNIL.
- Voir les Guidelines sur les DPIA du G29.

17 Gestion des incidents et des violations de données

Objectifs : disposer d'une organisation opérationnelle permettant de détecter et de traiter les événements susceptibles d'affecter les libertés et la vie privée des personnes concernées (définition des responsabilités, plan de réaction, qualifier les violations, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques :

- Définir les rôles et responsabilités des parties prenantes, ainsi que les procédures de remontées d'informations et de réaction, en cas de violation de données.
  - ♦ *Recommandations : formaliser les responsabilités du référent « Informatique et libertés » (CIL, DPO ou équivalent), les interactions avec la CNIL, les personnes concernées, la constitution d'une cellule de crise en cas de sinistre.*
- Établir un annuaire des personnes en charges de gérer les violations de données.
- Élaborer un plan de réaction en cas de violation de données pour chaque risque élevé, le tenir à jour et le tester périodiquement.
  - ♦ *Recommandations : tester le plan au moins une fois tous les deux ans.*
- Permettre de qualifier les violations de données selon leur impact sur les droits et libertés des personnes concernées.
  - ♦ *Recommandations : un simple événement est une violation de données sans conséquence, un incident correspond à une violation de données avec des conséquences isolées, un sinistre à une violation de données avec des conséquences immédiates importantes pour une ou plusieurs personnes, une crise à une violation de données avec des conséquences importantes et à plus long terme sur une ou plusieurs personnes.*
- Traiter les événements selon leur qualification (événement, incident, sinistre, crise, etc.). ♦ *Recommandations*
  - ◊ *s'il s'agit d'un événement, le consigner et avertir le référent « Informatique et libertés » (CIL, DPO ou équivalent) ;*
  - ◊ *s'il s'agit d'un incident, le résoudre en plus et, le cas échéant, notifier les personnes concernées par la violation (la notification d'une violation des données n'est pas nécessaire si la violation ne présente pas un risque élevé pour les droits et libertés des personnes, si le responsable de traitement a prouvé, à la satisfaction de l'autorité compétente, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.) ;*
  - ◊ *s'il s'agit d'un sinistre, déclencher en plus le lancement d'une analyse approfondie ;*
  - ◊ *s'il s'agit d'une crise, déclencher en plus un plan de gestion préalablement établi.*

- Tenir à jour une documentation des violations de données tel que prévu par l'article 33-5 du règlement général sur la protection des données (RGPD).
    - ♦ *Recommandations : consigner le contexte des violations de données, les catégorie de personnes et d'enregistrements concernés, le volume de personnes et d'enregistrement concernés, les effets de la violation, les mesures prises pour y remédier.*
- Étudier la possibilité d'améliorer les mesures de sécurité en fonction des violations de données qui ont eu lieu.

Notes

- Le « Paquet télécom » adopté par le Parlement européen en 2009 et transposé en droit français en 2011 crée une obligation de notifier certaines violations de données à la CNIL. Cette obligation est généralisée à tous les responsables de traitements et pas uniquement les « fournisseurs de services de communications électroniques accessibles au public » par le RGPD.devant entrer en vigueur en mai 2018. Ces textes définissent la forme des notifications :
    - ♦ la notification des personnes concernées, dans le cas où la dite violation engendre un risque élevé pour les droits et libertés des personnes, décrit au minimum la nature de la violation de données et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données;
    - ♦ la notification faite à l'autorité nationale compétente (la CNIL en France) décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier. Dans le cadre du RGPD, cette notification est nécessaire dès lors que la violation engendre un risque pour les droits et libertés des personnes.
    - ♦ Cette obligation n'est pas exclusive et n'annule pas les obligations de notification présentes au sein des autres textes nationaux ou européens.
- Il est important d'être en capacité de recueillir, conserver et présenter des preuves lorsqu'une action en justice est engagée suite à un incident.

Outillage / Pour aller plus loin

- Voir la procédure CLUSIF Victime.
- Voir la note CERTA Intrusion.
- Voir la Directive-2009-136.
- Voir les articles 33 et 24 du RGDP.

18 Gestion des personnels

Objectifs : diminuer la possibilité que les caractéristiques des personnes (employés, personnes ne faisant pas partie de l'organisme mais placées sous sa responsabilité) soient exploitées pour porter atteinte aux données (ressources et compétences adéquates, sensibilisation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les personnes ayant accès aux données et au traitement sont aptes à exercer leur fonction.
  - ♦ *Recommandations : vérifier que les personnes ont des compétences appropriées aux conditions d'exercice de leurs fonctions ou sinon prévoir des formations.*
- S'assurer que les conditions de travail des personnes ayant accès aux données et au traitement sont satisfaisantes.
  - ♦ *Recommandations : veiller à ce que les ressources (capacités de travail et disponibilités) soient suffisantes pour les tâches assignées.*
- Sensibiliser les personnes ayant accès aux données et au traitement aux risques liés à l'exploitation de leurs vulnérabilités.
  - ♦ *Recommandations : expliquer aux personnes que le fait qu'elles soient peu discrètes (loquaces, sans réserve, etc.), routinières (habitudes facilitant l'espionnage récurrent), influençables (naïves, crédules, obtuses, faible estime de soi, faible loyauté, etc.) ou manipulables (vulnérables face à la pression sur elles-mêmes ou leur entourage) peut être utilisé par des personnes mal intentionnées pour porter atteintes aux données.*

Outillage / Pour aller plus loin

- Dans certains cas, il convient également de mettre en œuvre des mesures d'accompagnement du changement (nouveaux services, nouveaux outils, nouvelles méthodes de travail, etc.) pour les personnes ayant accès aux données et au traitement.

19 Gestion des postes de travail

19.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des logiciels (systèmes d'exploitation, applications métiers, logiciels bureautiques, paramétrages, etc.) ne soient exploitées pour porter atteinte aux données à caractère personnel (mises à jour, protection physique et des accès, travail sur un espace réseau sauvegardé, contrôleurs d'intégrité, journalisation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Assurer la mise à disposition et le maintien en conditions opérationnelles et de sécurité des postes de travail des utilisateurs par le service en charge de l'informatique.
- Protéger les postes peu volumineux, donc susceptibles d'être facilement emportés, et notamment les ordinateurs portables, à l'aide d'un câble physique de sécurité, dès que l'utilisateur ne se trouve pas à proximité et que le local n'est pas sécurisé physiquement.
- Récupérer les données, à l'exception des données signalées comme privées ou personnelles, présentes sur un poste préalablement à sa réaffectation à une autre personne.
- Effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ou pour les postes partagés.
- Supprimer les données temporaires à chaque reconnexion des postes partagés.
- En cas de compromission d'un poste, rechercher toute trace d'intrusion dans le système afin de détecter si l'attaquant a compromis d'autres éléments.
- Tenir les systèmes et applications à jour (versions, correctifs de sécurité, etc.) ou, lorsque cela est impossible (ex : application uniquement disponible sur un système qui n'est plus maintenu par l'éditeur), isoler la machine et porter une attention particulière aux journaux.
    - ♦ *Recommandations : utiliser des versions maintenues par le constructeur ou un service tiers, mettre les logiciels à jour sans délai en programmant une vérification automatique hebdomadaire, tester les mises à jour avant de les déployer sur l'ensemble du système, s'assurer que les mises à jour soient réversibles en cas d'échec de leur application, vérifier régulièrement que les licences des logiciels sont valables, etc.*
- Documenter les configurations et les mettre à jour à chaque changement notable.

♦ *Recommandations : les modes opératoires liés au renforcement des ressources informatiques sont décrits, les liens nécessaires pour assurer les mises à jour de sécurité lors de l'installation sont identifiés, etc.*

- Limiter les possibilités de détournements d'usages.
    - ♦ *Recommandations : gérer les droits d'accès unitaires selon la règle du « moindre privilège » (éviter notamment d'autoriser l'usage de fonctionnalités*

avancées si ce n'est pas nécessaire), gérer les attributions d'adresses IP publiques ou privées en fonction des besoins effectifs, désactiver ou supprimer les services qui ne sont pas strictement nécessaires, désactiver ou supprimer les comptes inutiles (compte invité, comptes de support éditeur par défaut, etc.), interdire l'accès logique aux ports de diagnostic et de configuration à distance, désactiver l'exécution automatique lors de l'insertion d'un périphérique amovible, démarrer uniquement sur le disque local ou la mémoire locale, etc.

- Protéger les accès.
  - ♦ *Recommandations : protéger la configuration système bas niveau (exemple : BIOS) par mot de passe, changer les mots de passe par défaut, verrouiller l'accès au système par un écran de veille protégé par mot de passe et se déclenchant au bout d'un délai d'inactivité (5 minutes pour les opérations de maintenance, 15 minutes au plus pour une utilisation courante), afficher les dates et heures de la dernière connexion lors de la connexion à un compte, etc.*
- Activer les mesures de protection offertes par le système et les applications.
  - ♦ *Recommandations : activer les mots de passe d'ouverture de session, le parefeu, la mise à jour automatique, la protection contre les programmes malveillants? quand le système d'exploitation le permet ; activer les contrôles d'accès aux applications quand elles en disposent, etc.*
- Interdire le partage de répertoires ou de données localement sur les postes de travail.
- Stocker les données des utilisateurs sur un espace réseau sauvegardé et non sur les postes de travail.
- Dans le cas où des données doivent être stockées en local sur un poste, fournir des moyens de synchronisation ou de sauvegarde aux utilisateurs et les informer sur leur utilisation.
  - ♦ *Recommandations : des espaces individuels sur les serveurs de fichiers avec un plan de classement explicite, des scripts automatiques de copie de dossiers locaux, des outils de synchronisation automatique gérés par le service en charge de l'informatique.*
- Sécuriser la configuration du navigateur Internet.
  - ♦ *Recommandations : la configuration doit inclure la protection des informations nominatives stockées par le navigateur (formulaires, mots de passe, certificats, etc.), l'utilisation d'un mot de passe principal sous Mozilla Firefox, l'impossibilité de stocker des mots de passe en cas de risques élevés, etc.*
- Déployer le navigateur dont la configuration a été sécurisée sur tous postes de travail nécessitant un accès à Internet ou Intranet.
- Limiter le recours à des modules d'extension (plugins), supprimer ceux qui ne sont pas utilisés et tenir à jour ceux qui sont installés.
- Interdire l'exécution des applications téléchargées ne provenant pas de sources sûres.
- Rechercher les vulnérabilités exploitables.

- ♦ *Recommandations : exercer une veille active concernant les vulnérabilités découvertes sur les logiciels utilisés dans le cadre du traitement, utiliser des outils de détection des vulnérabilités (logiciels scanners de vulnérabilités tels que nmap, nikto, etc.), voire des systèmes de détection et prévention des attaques (Host Intrusion Prevention), s'assurer que les principales vulnérabilités sont couvertes, etc.*

- Contrôler l'intégrité du système à l'aide de contrôleurs d'intégrité (qui vérifient l'intégrité de fichiers choisis).
  - ♦ *Recommandations : surveiller de façon permanente les modifications apportées à certains fichiers ou répertoires (utiliser des logiciels tels que Tripwire), contrôler la base de registre et les processus lancés par le système (utiliser des logiciels tels que Spybot), détecter la présence de rootkits (utiliser des logiciels tels que Rootkit Revealer), etc.*
- S'assurer que la taille maximale des journaux d'événements est suffisante, et notamment que les événements les plus anciens ne sont pas supprimés automatiquement si la taille maximale est atteinte.
- Journaliser les événements relatifs aux applications, à la sécurité et au système (voir la page Traçabilité (journalisation)).
  - ♦ *Recommandations : connexions au système (enregistrer l'identifiant, la date et l'heure de leur tentative de connexion, le fait que la connexion ait réussi ou non, ainsi que la date et l'heure de la déconnexion), modification de paramètres de sécurité, de privilèges, de comptes utilisateurs et de groupes, événements système (arrêt / redémarrage de processus système sensibles), accès / modification de données système, échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.), exécution de transactions sensibles, l'application des correctifs de sécurité, actions d'administration et de prise de main à distance, journaux du logiciel antivirus (activation/désactivation, mises à jour, détection de codes malveillants, etc.), etc.*
- Exporter les journaux à l'aide des fonctionnalités de gestion du domaine ou via un client syslog.
- Analyser principalement les heures de connexions et déconnexions, le type de protocole utilisé pour se connecter et le type d'utilisateur qui y a recours, l'adresse IP d'origine de la connexion, les échecs successifs de connexions, les arrêts inopinés d'applications ou de tâches.

Outillage / Pour aller plus loin

- Selon la nature de l'application, il peut être nécessaire d'assurer l'intégrité, la disponibilité et si besoin la confidentialité des logiciels et des codes sources des applications développées en interne, notamment si elles sont rares, novatrices ou ont une grande valeur marchande, par le recours à des signatures du code exécutable garantissant qu'il n'a subi aucune altération. À cet égard, une vérification de signature tout au long de l'exécution (et pas seulement avant l'exécution) rend plus difficile la compromission d'un programme.

19.2 Spécificités pour les postes nomades

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des postes nomades (PC portables, assistants personnels, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données stockées sur les postes nomades.
  - ♦ *Recommandations : chiffrement du disque dur dans sa totalité au niveau matériel, chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation, chiffrement fichier par fichier, création de conteneurs chiffrés, etc.*
- Limiter le stockage de données sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors de déplacement à l'étranger.
- Assurer la disponibilité des données stockées sur les postes nomades.
  - ♦ *Recommandations : les copier dès que possible sur un autre poste, sur un serveur.*
- Purger les données collectées sur le poste nomade sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
- Positionner un filtre de confidentialité sur les écrans des postes nomades dès qu'ils sont utilisés en dehors de l'organisme.

Notes

- De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL.
- Il convient de ne pas désactiver le chiffrement de disque et de veiller à conserver une copie des clés quand le chiffrement est disponible.

Outillage / Pour aller plus loin

- Voir le guide ANSSI Voyageurs pour les voyages à l'étranger.

19.3 Spécificités pour les téléphones mobiles / *smartphones*

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des téléphones mobiles / *smartphones*.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Configurer les téléphones avant d'être livrés aux utilisateurs.
  - ♦ *Recommandations : il faut que les téléphones soient verrouillés automatiquement après une période d'inactivité (1 à 5 minutes), la carte*

mémoire (microSD) sur laquelle les courriers électroniques sont stockés doit être chiffrée, le verrou distant doit être activé afin de pouvoir effacer le contenu en cas de perte ou de vol, l'installation de nouvelles applications est limitée (si possible).

- Informer les utilisateurs, par exemple sous la forme d'une note accompagnant la livraison, sur l'usage du téléphone, des applications (ex : business mail, Exchange, etc.) et des services fournis, ainsi que sur les règles de sécurité à respecter.
    - ♦ *Recommandations : les utilisateurs ne doivent pas diminuer le niveau de sécurité en modifiant la configuration du téléphone, ils ne doivent pas ouvrir les courriers d'origine inconnue, ils ne doivent pas stocker de fichiers sensibles (en dehors de la lecture des courriers), ils doivent effacer régulièrement le cache et les cookies, ils doivent immédiatement avertir le service en charge de l'informatique en cas d'incident, ils ne doivent pas installer de logiciels sur l'appareil, sauf s'ils proviennent d'une source de confiance (vérifier la réputation avant d'installer ou d'utiliser des applications ou des services) envoyant un contenu qu'ils s'attendent à recevoir.*
- Sécuriser le serveur.
    - ♦ *Recommandations : isoler le serveur du reste du réseau dans une DMZ spécifique ou un VLAN, utiliser un anti-virus à jour, un anti-spyware et un anti-spam, installer immédiatement les mises à jour de sécurité du système d'exploitation, authentifier les appareils par certificat électronique (si possible).*
- Sécuriser la fin de vie de l'appareil.
    - ♦ Recommandations : avant élimination ou recyclage du téléphone, effacer toutes les données et les paramètres, appliquer une procédure approfondie de démantèlement, y compris d'effacement de la mémoire.

Outillage / Pour aller plus loin

- Voir l'article CNIL Smartphones.
- Voir le guide CLUSIF Voix.
- Voir le rapport ENISA Smartphone.
- Des mesures plus rigoureuses peuvent être envisagées si les risques sont jugés trop importants (bloquer les pièces jointes, tracer et vérifier les flux avec une sonde, vérifier l'effectivité du chiffrement, ne pas stocker des données sensibles au niveau local et ne permettent qu'un accès en ligne à des données sensibles à partir d'un smartphone grâce à une application non-mise en cache, ne pas envoyer de fichiers sensibles sur les smartphones par courrier électronique en cas de risques élevés, utiliser un logiciel de chiffrement de confidentialité SMS de bout en bout, définir une liste blanche d'applications utilisables, ré-installer régulièrement une image du disque spécialement préparée et testée.).

20 Gestion des projets

Objectifs : prendre en compte la protection des données à caractère personnel dans tout nouveau traitement (labels de confiance, référentiels, gestion de risques CNIL, formalités CNIL, etc.).

20.1 Mesures génériques

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser la démarche de gestion des risques de la CNIL dès l'élaboration d'un service ou la conception d'une application.
- Privilégier le recours à des labels de confiance dans les domaines de la SSI et « Informatique et libertés » (procédures, produits, systèmes de management, organismes, personnes, etc.).
    - ♦ *Recommandations : une certification de sécurité de premier niveau, une qualification (au niveau standard, renforcé ou élevé), une certification en vertu du décret n°2002-535 du 18 avril 2002, selon sept niveaux d'assurance croissante, un agrément ou caution (jugeant de l'aptitude à assurer la protection d'informations classifiées de défense ou d'informations sensibles non classifiées de défense), une certification de système de management de la sécurité de l'information ISO-27001, une certification de personne dans le domaine de la SSI*
      (CISSP ? Certified Information Systems Security Professional, CISM ? Certified Information Security Manager, ISO 27001 Lead Auditor, etc.).
- Privilégier le recours à des référentiels éprouvés et reconnus.
    - ♦ *Recommandations : Recourir de préférence à des normes internationales, des guides publiés par des institutions (CNIL, ANSSI, etc.).*
- Effectuer les formalités CNIL avant le lancement d'un nouveau traitement.

Outillage / Pour aller plus loin

- Voir les principes « Adapter la SSI selon les enjeux », « Utiliser des produits et prestataires labellisés pour leur sécurité » et « Des efforts proportionnés aux enjeux SSI » du référentiel général de sécurité (RGS).
- Voir les règles et recommandations relatives aux « Accusé d'enregistrement et accusé de réception » du RGS et les annexes associées.
- Voir les catalogues de produits labellisés par l'ANSSI.
- Voir les guides ANSSI Maturité SSI et ANSSI GISSIP.

20.2 Spécificités pour les acquisitions de logiciels (achats, développements, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Vérifier que les développeurs et les mainteneurs disposent des ressources suffisantes pour maîtriser leurs actions.
    - ♦ Recommandations : vérifier l'existence de spécifications claires, d'une documentation adéquate, des compétences suffisantes.
- Privilégier les applications interopérables et ergonomiques.
- Effectuer les développements informatiques dans un environnement informatique distinct de celui de la production
    - ♦ *Recommandations : effectuer les développements sur des ordinateurs différents et dans des salles différentes du système en production.*
- Protéger la disponibilité, l'intégrité et si besoin la confidentialité des codes sources.
- Imposer des formats de saisie et d'enregistrement des données qui minimisent les données collectées.
    - ♦ *Recommandations : s'il s'agit de collecter l'année de naissance d'une personne, le champ du formulaire correspondant ne doit pas permettre la saisie du mois et du jour de naissance (mise en œuvre d'un menu déroulant limitant les choix pour un champ d'un formulaire).*
- S'assurer que les formats de données sont compatibles avec la mise en œuvre d'une durée de conservation.
- Intégrer le contrôle d'accès aux données par des catégories d'utilisateurs au moment du développement.
- Éviter le recours à des zones de texte libre, et si de telles zones sont requises, faire apparaître soit en filigrane, soit comme texte pré-rempli s'effaçant sitôt que l'utilisateur décide d'écrire dans la zone, les mentions suivantes : « Les personnes disposent d'un droit d'accès aux informations contenues dans cette zone de texte. Les informations que vous y inscrivez doivent être PERTINENTES au regard du contexte. Elles ne doivent pas comporter d'appréciation subjective, ni faire apparaître, "directement ou indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelles de celles-ci" ».
- Interdire l'utilisation de données réelles avant la mise en opération, et les anonymiser si nécessaire.
    - ♦ *Recommandations : anonymiser les données de production lors des tests de recette, effacer de manière sécurisée tout support ayant servi à stocker des données sensibles (voir la page Anonymisation)*
- Vérifier que les logiciels fonctionnent correctement et conformément lors de la recette.

Outillage / Pour aller plus loin

- Voir le référentiel général d'interopérabilité.

21 Gestion des risques

Objectifs : maîtriser les risques que les traitements de l'organisme font peser sur les droits et libertés des personnes concernées (recensement des traitements de données à caractère personnel, des données, des supports, appréciation des risques, déterminer les mesures existantes ou prévues, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Recenser les traitements de données à caractère personnel, automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels ils reposent :
  - ♦ les matériels (ex : serveur de gestion des ressources humaines, ordinateur portable, CD-ROM) ;
  - ♦ les logiciels (ex : système d'exploitation, logiciel métier) ;
  - ♦ les canaux de communication (ex : fibre optique, Wifi, Internet) ; ♦ les supports papier (ex : document imprimé, photocopie).
- Évaluer la manière dont les principes fondamentaux (information, consentement, droit d'accès...) sont respectés.
- Apprécier les risques de chaque traitement.
  - ♦ Identifier les impacts potentiels (quels pourraient être les conséquences sur les droits et libertés des personnes concernées ?) pour les trois risques suivants :
    - ◊ Accès illégitime à des données (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
    - ◊ modification non désirée de données (ex : accusation à tort d'une personne suite à la modification des journaux d'accès) ;
    - ◊ disparition de données (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).
  - ♦ Identifier les sources de risques (qui ou quoi pourrait être à l'origine de chaque risque ?), en prenant en compte :
    - ◊ les sources humaines internes et externes, de manière accidentelle ou délibérée (ex : administrateur informatique, utilisateur, attaquant externe, concurrent) ;
    - ◊ les sources non humaines internes ou externes (ex : eau, matériaux dangereux, virus informatique non ciblé).
  - ♦ Identifier les menaces réalisables (qu'est-ce qui pourrait permettre que chaque risque survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papier, etc.), qui peuvent être :

- ◊ utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;
- ◊ modifiés (ex : piégeage logiciel ou matériel ? *keylogger*, installation involontaire d'un logiciel malveillant) ;
- ◊ perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;
- ◊ observés (ex : d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel) ;
- ◊ détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;
- ◊ surchargés (ex : unité de stockage pleine, attaque par dénis de service).

♦ Déterminer les mesures existantes ou prévues (techniques et organisationnelles) qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).

♦ Estimer la gravité et la vraisemblance des trois risques, au regard des éléments précédents, compte tenu des mesures existantes ou prévues (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

♦ *Recommandations : le tableau suivant peut être utilisé pour formaliser cette réflexion :*

Risques	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

- Mettre en œuvre et vérifier les mesures prévues. Si les mesures existantes et prévues sont jugées comme appropriées afin de garantir un niveau de sécurité adapté aux risques, il convient de s'assurer qu'elles soient appliquées et contrôlées.
- Faire réaliser des audits de sécurité périodiques, si possible annuels. Chaque audit devrait donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.
- Ajuster la cartographie à chaque évolution majeure et de manière périodique.

♦ *Recommandations : quand un nouveau traitement est créé, et au moins une fois par an au sein d'un comité dédié.*

Outillage / Pour aller plus loin

- Le règlement n°2016/679 du 27 avril 2016 introduit la notion d' « analyse d'impact relative à la protection des données » et précise que celle-ci doit au moins contenir « *une description du traitement et de ses finalités, une évaluation de la nécessité et de la proportionnalité, une appréciation des risques sur les droits et libertés des personnes concernées, et les mesures envisagées pour traiter ces risques et se conformer au règlement* » (cf. article 35.7). La réflexion sur les risques dont il est question dans la présente fiche permet d'alimenter l'analyse d'impact.
- L'emploi d'une véritable méthode permet de disposer d'outils pratiques et d'améliorer l'exhaustivité et la profondeur de l'étude des risques. À cet effet, les guides PIA (*Privacy Impact Assessment*) de la CNIL permettent de mener une analyse d'impact relative à la protection des données.
- L'étude des risques sur la sécurité de l'information peut être menée en même temps que l'étude des risques sur la vie privée. Les approches étant compatibles, il n'est pas difficile de les factoriser.
- L'étude des risques permet de déterminer des mesures techniques et organisationnelles à mettre en place. Il convient donc de prévoir un budget pour leur mise en œuvre .
- Voir le référentiel général de sécurité (RGS).
- Voir la méthode EBIOS.

22 Information des personnes concernées (traitement loyal et transparent)

22.1 Mesures génériques

Objectifs : être conforme à l'article 32 de la loi informatique et libertés et les articles 12, 13 et 14 du règlement général sur la protection des données (RGPD) ; garantir l'information des personnes et donc éviter la collecte de données à leur insu ; vérifier que le traitement ne fait pas l'objet d'une exception ou de conditions particulières mentionnées dans l'article 32 de la loi informatique et libertés (utilisateur des réseaux de communication électronique, statistiques, anonymisation, sûreté de l'État, défense, sécurité publique, exécution de condamnations pénales, mesures de sûreté, prévention, recherche, constatation ou poursuite d'infractions pénales).

Bonnes pratiques

- Déterminer et justifier les moyens pratiques qui vont être mis en œuvre pour informer les personnes concernées, ou justifier de l'impossibilité de leur mise en œuvre :
  - ♦ présentation des conditions d'utilisation/confidentialité ;
  - ♦ possibilité d'accéder aux conditions d'utilisation/confidentialité ;
  - ♦ conditions lisibles et compréhensibles ;
  - ♦ existence de clauses spécifiques au dispositif ;
  - ♦ présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.) ;
  - ♦ présentation détaillée des données personnelles collectées ;
  - ♦ présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers ;
  - ♦ présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.) ;
  - ♦ information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation ;
  - ♦ modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité ;
  - ♦ le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité ;
  - ♦ Dans le cas de transmission de données à des tiers :
    - ◊ présentation détaillée des finalités de transmission à des tiers ;
    - ◊ présentation détaillée des données personnelles transmises ;
    - ◊ indication de l'identité des entreprises tierces.
- S'assurer que l'information sera réalisée de manière complète, claire et adaptée au public visé, en fonction de la nature des données et des moyens pratiques choisis.

- ♦ *Recommandations : formuler l'information dans un langage compréhensible du point de vue d'une personne non formée aux technologies informatiques ou de l'Internet.*

- S'assurer que l'information sera réalisée au plus tard au moment où seront collectées les données.
- S'assurer que la collecte ne puisse pas être effectuée sans information.
  - ♦ *Recommandations : déterminer des solutions alternatives au cas où les moyens pratiques choisis ne seraient plus opérationnels.*
- Si possible, prévoir un moyen de prouver que l'information a été faite.
  - ♦ *Recommandations : placer l'information sur un panneau que tous les employés ont forcément vu, faire signer un émargement ou un document...*

Notes

- L'information doit être individuelle (échange verbal, fenêtre pop-up?), mais peut être collective (note, affichette dans un local?) si le responsable de traitement est certain que toutes les personnes concernées auront accès facilement au moyen d'information.
- L'information doit porter sur l'identité du responsable de traitement, la finalité du traitement, le caractère obligatoire ou facultatif des informations collectées, les conséquences en cas de défaut de réponse, les destinataires de ces informations, les droits et la personne auprès de qui les faire valoir, et les transmissions envisagées.
- Attention : dans le cas de transmission de données à des sociétés tierces au responsable du traitement (filiales, affiliés, intragroupe, partenaires, etc.), il est nécessaire de fournir la liste des destinataires (dans une rubrique d'information dédiée), en précisant les catégories de données transmises et la finalité du transfert, et en fournissant un lien hypertexte vers la politique de protection des données des destinataires respectifs. Il faut également prévoir un processus interne permettant de mettre à jour cette liste en cas de modification.

Outillage / Pour aller plus loin

- Voir l'article 32 de la loi informatique et libertés et les articles 12, 13 et 14 du RGPD pour le contenu de l'information, les exceptions et les conditions particulières.
- Voir les modèles de mentions légales sur le site de la CNIL (https://www.cnil.fr/fr/modeles/mention).
-

22.2 Spécificités pour les salariés d'un organisme

Bonnes pratiques

- Obtenir l'avis préalable des institutions représentatives du personnel dans les cas prévus par le Code du travail.

- Utiliser le moyen le plus approprié à la culture de l'organisme.
    - ♦ *Recommandations : affichage, note interne, courrier électronique, formulaire spécifique, contrat de travail, règlement intérieur, charte informatique?*

22.3 Spécificités pour une collecte de données via un site Internet

Bonnes pratiques

- Faire figurer une information à destination des internautes directement ou facilement accessible.
    - ♦ *Recommandations : afficher ou rendre accessible l'information sur la page d'accueil, ou au sein de la rubrique du site ou du service consulté traitant du respect de la vie privée?*

22.4 Spécificités pour une collecte de données via un objet connecté ou une application mobile

Bonnes pratiques

- Faire figurer une information à destination des utilisateurs directement ou facilement accessible.
    - ♦ *Recommandations : afficher un message au premier démarrage de l'objet ou de l'application mobile, et rendre l'information accessible ensuite par un menu spécifique ; placer un « QR Code » d'information sur l'objet s'il n'a pas d'écran.*
- Informer l'utilisateur si l'application est susceptible d'accéder à des identifiants de l'appareil, en précisant s'ils sont communiqués à des tiers.
- Informer l'utilisateur si l'application est susceptible de fonctionner en arrière-plan.
- Présenter à l'utilisateur les protections d'accès à l'appareil.

22.5 Spécificités pour une collecte de données par téléphone

Bonnes pratiques

- Délivrer un message automatique avant que la conversation soit engagée, précisant notamment les droits des personnes, et le cas échéant, les finalités de l'enregistrement de la conversation (formation, enquête sur la qualité du service rendu, etc.), en leur offrant la possibilité de s'opposer à l'enregistrement (pour motif légitime).
- Mettre en place des moyens permettant l'authentification de l'appelant (ex : par une information connue seulement de l'organisme et de la personne concernée).

22.6 Spécificités pour une collecte de données via un formulaire

Bonnes pratiques

• Placer la mention appropriée sur le formulaire avec une typographie identique au reste du document.

22.7 Spécificités pour l'utilisation de techniques de publicité ciblée

Bonnes pratiques

- Rendre accessible l'information des internautes de manière à ce qu'elle soit parfaitement visible et lisible.
- Informer les internautes sur les différentes formes de publicité ciblée auxquelles ils sont susceptibles d'être exposés via le service qu'ils consultent et les divers procédés utilisés, les catégories d'informations traitées aux fins d'adapter le contenu publicitaire et, en tant que de besoin, les informations non recueillies, leurs possibilités pour consentir à l'affichage de publicités comportementales ou personnalisées. L'information et le recueil du consentement doivent être effectués avant tout stockage d'information ou obtention de l'accès à des informations déjà stockées dans l'équipement terminal.

Outillage / Pour aller plus loin

- Voir l'avis G29-Publicité.

22.8 Spécificités pour la mise à jour d'un traitement existant

Bonnes pratiques

• Informer plus particulièrement sur les nouveautés du traitement (nouvelles finalités, nouveaux destinataires?).

23 Lutte contre les logiciels malveillants

Objectifs : protéger les accès vers des réseaux publics (Internet) ou non maîtrisés (partenaires), ainsi que les postes de travail et les serveurs contre les codes malveillants qui pourraient affecter la sécurité des données à caractère personnel (antivirus, firewall, proxy, anti-spyware, remontée des événements de sécurité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Installer un antivirus sur les serveurs et postes de travail et le configurer
  - ♦ *Recommandations : assurer une analyse en temps réel du système selon les règles définies par le service en charge de l'informatique, l'utilisateur ne doit pas pouvoir désactiver l'antivirus de son poste ni modifier ses paramètres, réaliser une analyse complète des disques locaux au moins de façon hebdomadaire et automatique tout en perturbant au minimum le fonctionnement du service (par exemple en heures creuses ou en limitant la charge système allouée à l'analyse, ou en heures non ouvrées, etc.).*
- Tenir les logiciels antivirus à jour.
  - ♦ *Recommandations : déployer automatiquement les mises à jour des bases antivirales et des moteurs d'antivirus sur les serveurs et les postes de travail de manière régulière et pouvoir réaliser des mises à jour d'urgence.*
- Mettre en œuvre des mesures de filtrage permettant de filtrer les flux entrants/sortants du réseau (firewall, proxy, etc.).
- Faire remonter les événements de sécurité de l'antivirus sur un serveur centralisé pour analyse statistique et gestion des problèmes a posteriori (dans le but de détecter un serveur infecté, un virus détecté et non éradiqué par l'antivirus, etc.).
- Installer un programme de lutte contre les logiciels espions (anti-spyware) sur les postes de travail, le configurer et le tenir à jour.

Outillage / Pour aller plus loin

- Voir la note rappel sur les virus et chevaux de Troie du CERTA.
- Voir la note rappel sur les virus de messageriedu CERTA.

24 Maintenance

24.1 Mesures génériques

Objectifs : limiter la vraisemblance des menaces liées aux opérations de maintenance sur les matériels et logiciels (contrat de sous-traitance, télémaintenance, accord de l'utilisateur, effacement des données, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Encadrer par un contrat de sous-traitance la réalisation des opérations de maintenance lorsqu'elles sont effectuées par des prestataires (voir la page Relations avec les tiers).
- Enregistrer toutes les opérations de maintenance dans une main courante.
- Encadrer les opérations de télémaintenance.
    - ♦ *Recommandations : utiliser systématiquement des canaux de communications chiffrés, utiliser des mots de passe ou des clés d'authentification robustes, journaliser les accès (voir la page Traçabilité (journalisation)).*
- Chiffrer ou effacer les données présentes sur les matériels (poste de travail fixe ou nomades, serveurs, etc.) envoyés en maintenance externe. En cas d'impossibilité déposer les supports de stockage de l'équipement avant l'envoi en maintenance ou gérer la maintenance en interne.

24.2 Spécificités pour les postes de travail (ordinateurs fixes et mobiles, *smartphones*, tablettes)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Lors des opérations de maintenance nécessitant une prise en main à distance sur un poste de travail, ne réaliser l'opération qu'après avoir obtenu l'accord de l'utilisateur, et lui indiquer à l'écran si la prise en main est effective.
- Lorsqu'une opération de maintenance nécessite une intervention physique sur un poste de travail contenant des données sensibles au sens de l'article 8 de la loi informatique et libertés et des données relevant de l'article 9 de la même loi, supprimer les données pendant la maintenance.
- Configurer les téléphones via avant de les remettre aux utilisateurs.
    - ♦ *Recommandations : il faut que les téléphones soient verrouillés automatiquement après une période d'inactivité (1 à 5 minutes), la carte mémoire (microSD) sur laquelle les courriers électroniques sont stockés doit être chiffrée, le verrou distant doit être activé afin de pouvoir effacer le contenu en cas de perte ou de vol, l'installation de nouvelles applications est*

limitée (si possible), et l'ensemble de ces mesures doit être gérée par un système de gestion de flotte permettant de forcer l'application de ces règles.

- Informer les utilisateurs, par exemple sous la forme d'une note accompagnant la livraison, sur l'usage du téléphone, des applications (ex : *business mail, Exchange?*) et des services fournis, ainsi que sur les règles de sécurité à respecter.
    - ♦ *Recommandations : les utilisateurs ne doivent pas ouvrir les courriers d'origine inconnue, ils ne doivent pas stocker de fichiers sensibles (en dehors de la lecture des courriers), ils doivent effacer régulièrement le cache et les cookies, ils doivent immédiatement avertir le service en charge de l'informatique en cas de perte, de vol ou de comportement anormal du téléphone, ils ne doivent pas installer de logiciels sur l'appareil, sauf s'ils proviennent d'une source de confiance (vérifier la réputation avant d'installer ou d'utiliser des applications ou des services) envoyant un contenu qu'ils s'attendent à recevoir, etc.*
- Sécuriser la fin de vie de l'appareil.
    - ♦ *Recommandations : avant élimination ou recyclage du poste de travail, effacer toutes les données et les paramètres, appliquer une procédure approfondie de démantèlement, y compris d'effacement de la mémoire, etc.*

24.3 Spécificités pour les supports de stockage

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effacer de façon sécurisée ou bien détruire physiquement les supports de stockage mis au rebut.
    - ♦ *Recommandation : effacer les supports de stockage magnétiques (disques durs, bandes, etc.) à l'aide de logiciels d'effacement sécurisés (consulter notamment la liste des logiciels d'effacement certifiés par l'ANSSI) ou bien d'un dégausseur, ou bien faire appel à un prestataire spécialisé dans la destruction de supports de stockage.*
- Lors des opérations de maintenance nécessitant une prise en main à distance sur un poste de travail, ne réaliser l'opération qu'après avoir obtenu l'accord de l'utilisateur.

24.4 Spécificités pour les imprimantes et copieurs multifonctions

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données.
    - ♦ *Recommandations : les données doivent être chiffrées ou effacées de manière sécurisée avant l'envoi en maintenance externe ; faire signer un engagement de confidentialité au mainteneur ou faire des réparations sur place en présence d'un membre du service en charge de l'informatique si les données sont sensibles et si elles ne peuvent pas être chiffrées ou effacées dans leur*

totalité (panne d'un disque dur, dysfonctionnement, etc.) ; interdire l'envoi en maintenance externe dans le cas de données sensibles, etc.

- Dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès.
  - ♦ *Recommandations : faire signer un engagement de confidentialité par le tiers externe, mettre en place de mots de passe robustes, spécifiques et renouvelés régulièrement, pour l'accès en télémaintenance, activer les accès entrant en télémaintenance uniquement sur demande, les accès entrant étant inactifs par défaut, journaliser les accès en télémaintenance, interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers internet, etc.*
- Empêcher l'accès à des données stockées sur des imprimantes ou copieurs multifonctions mis au rebut.
  - ♦ *Recommandations : entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès-verbal de destruction des supports et le conserver pendant 10 ans.*

25 Minimisation des données : adéquates, pertinentes et limitées

25.1 Minimisation de la collecte

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(c) du règlement général sur la protection des données (RGPD) ; réduire la gravité des risques en limitant la collecte des données à caractère personnel au strict nécessaire au regard d'une finalité définie ; éviter la collecte de données non nécessaires, l'utilisation de données sans lien avec la finalité et des impacts excessifs pour les personnes.

Bonnes pratiques

- Justifier de la collecte de chaque donnée.
- Bien faire la distinction entre les données anonymes et pseudonymes.
- Éviter les champs de saisie en texte libre (ex : zones « commentaires »), en raison du risque que les utilisateurs y consignent des informations ne respectant pas les principes de minimisation. On préférera donc des champs de saisie à base de listes déroulantes. Si on ne peut éviter la saisie de texte libre, une sensibilisation des utilisateurs devra être faite quant à l'usage de ces champs, vis-à-vis des conditions générales du service et vis-à-vis de la loi (pas de propos injurieux, pas de données sensibles non déclarées, etc.).

- Vérifier que les données sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie, et ne pas les collecter dans le cas contraire.
    - ♦ *Recommandations : définir la finalité du traitement, puis identifier les données nécessaires à cette finalité et justifier en quoi chaque catégorie de données est indispensable, et enfin écarter toute données qui ne rend pas la finalité irréalisable ; si besoin, revoir la finalité si des données sont nécessaires à autre chose que la finalité initialement prévue.*
- Vérifier que les données ne font pas apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle, et ne pas les collecter dans le cas contraire à moins d'être dans des circonstances d'exception (consentement, intérêt public? conformément à l'article 8 de la loi informatique et libertés et à l'article 9 du RGPD).
- Vérifier que les données ne sont pas relatives à des infractions, condamnations ou mesures de sûreté, et ne pas les collecter dans le cas contraire, à moins d'être dans des circonstances d'exception (juridictions, auxiliaires de justice? conformément à l'article 9 de la loi informatique et libertés et à l'article 10 du RGPD).
- Empêcher de collecter davantage de données.
    - ♦ *Recommandations : seuls les champs relatifs aux données déterminées sont créés et peuvent être renseignés dans une base de données et aucun autre champ ne peut être ajouté (ne pas prévoir de champ « texte libre » mais des listes déroulantes ; si on ne peut éviter la saisie de texte libre, mettre en garde les utilisateurs), vérifier régulièrement qu'aucune données supplémentaire n'a été collectée par rapport à ce qui était initialement prévu?*

Notes

- Certaines catégories de données font l'objet de contraintes particulières (en particulier les données dites « sensibles » et les données « relatives aux infractions, condamnations et mesures de sûreté », dont le traitement ne peut être mis en œuvre que par certaines catégories de personnes morales, selon les articles 8 et 9 de la loi informatique et libertés et les article 9 et 10 du RGPD).
- En raison du caractère sensible des données relatives à un mineur et en tenant compte du principe de loyauté de collecte vis-à-vis d'un utilisateur vulnérable, la collecte de données concernant un enfant, ses parents ou sa famille devra être particulièrement limitée et justifiée.

25.2 Minimisation des données elles-mêmes

Objectifs être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(c) du RGPD ; réduire la gravité des risques en minimisant les données elles-mêmes, par des mesures destinées à réduire leur sensibilité.

Bonnes pratiques

- Filtrer et retirer les données inutiles.
  - ♦ *Recommandations : lors de l'importation de données, différents types de métadonnées (par exemple, des données EXIF attachées avec un fichier d'image) peuvent être involontairement collectés. Ces métadonnées doivent être identifiées et éliminées si elles ne sont pas nécessaires aux finalités spécifiées.*
- Réduire la sensibilité par transformation.
  - ♦ *Recommandations : après réception de données sensibles, faisant partie d'un lot d'informations générales ou transmises à des fins statistiques uniquement, celles-ci peuvent être converties en une forme moins sensible ou pseudonymisée.*
    Par exemple :
    - ◊ *si le système collecte l'adresse IP pour déterminer l'emplacement de l'utilisateur dans un but statistique, l'adresse IP peut être supprimées après déduction de la ville ou du quartier ;*
    - ◊ *si le système reçoit des données vidéo à partir de caméras de surveillance, il peut reconnaître les personnes debout ou en mouvement dans la scène et les flouter ;*
    - ◊ *si le système est un compteur intelligent, il peut agréger l'utilisation de l'énergie sur une certaine période, sans l'enregistrer en temps réel.*
- Réduire le caractère identifiant des données (Voir la rubrique Anonymisation).
  - ♦ *Recommandations : le système peut faire en sorte que :*
    - ◊ *l'utilisateur peut utiliser une ressource ou un service sans risque de divulguer son identité (données anonymes) ;*
    - ◊ *l'utilisateur peut utiliser une ressource ou un service sans divulguer son identité, mais reste identifiable et responsable de cette utilisation (données pseudonymes) ;*
    - ◊ *l'utilisateur peut faire de multiples utilisations des ressources ou des services sans risque que ces utilisations puissent être reliées ensemble (données non corrélables) ;*
    - ◊ *l'utilisateur peut utiliser une ressource ou un service sans risque que d'autres, en particulier des tiers, puissent être en mesure d'observer que la ressource ou le service est utilisé (non-observabilité).*
  - ♦ *Le choix d'une méthode de la liste ci-dessus doit dépendre des menaces identifiées. Pour certains types de menaces sur la vie privée, la pseudonymisation sera plus appropriée que l'anonymisation (par exemple, s'il y a un besoin de traçabilité). En outre, certaines menaces sur la vie privée seront traitées par une combinaison de plusieurs méthodes.*
- Réduire l'accumulation de données.
  - ♦ *Recommandations : le système peut être structuré en parties indépendantes avec des fonctions de contrôle d'accès distinctes. Les données peuvent*

également être réparties entre ces sous-systèmes indépendants et contrôlées par chaque sous-système en utilisant différents mécanismes de contrôle d'accès. Si un sous-système est compromis, les impacts sur l'ensemble des données peuvent ainsi être réduits.

- Restreindre l'accès aux données.
  - ♦ *Recommandations : le système peut limiter l'accès aux données selon le principe du « besoin d'en connaître ». Le système peut séparer les données sensibles et appliquer des politiques de contrôle d'accès spécifiques. Le système peut aussi chiffrer les données sensibles pour protéger leur confidentialité lors de la transmission et du stockage. L'accès aux fichiers cachés temporaires qui sont produits au cours du traitement des données devrait également être protégé.*
- Limiter l'envoi des documents électroniques contenant des données aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Effacer de manière sécurisée les données qui ne sont plus utiles ou qu'une personne demande de supprimer, sur le système en opération et sur les sauvegardes le cas échéant (voir également la page Durées de conservation : limitées).
  - ♦ *Recommandations : utiliser un outil d'effacement sécurisé pour les documents électroniques, un « dégausseur » pour les unités de stockage à technologie magnétique...*

Outillage/Pour aller plus loin

- Voir la liste des produits ayant reçu une certification de sécurité de premier niveau (CSPN) de l'agence nationale de la sécurité des systèmes d'information (ANSSI) sur http://www.ssi.gouv.fr/).
- Voir le guide ANSSI-Effacement et les logiciels d'effacement sécurisé certifiés.

26 Organisation

Objectifs : disposer d'une organisation apte à diriger et contrôler la protection des données à caractère personnel au sein de l'organisme (désigner un CIL/DPO, créer un comité de suivi, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Faire désigner par le responsable des traitements une personne en charge de l'assister dans la mise en application de la loi informatique et libertés et du règlement général sur la protection des données (RGPD)t lui accorder les moyens nécessaires à l'exercice de sa mission.
    - ♦ *Recommandations : désigner un correspondant « Informatique et libertés » (CIL) / data Protection Officer (DPO), fixer ses missions dans une lettre de mission, lui attribuer les ressources humaines et financières, lui permettre d'exercer sa fonction directement auprès du responsable des traitements, avec une liberté organisationnelle et décisionnelle, en dehors de tout conflit d'intérêt, informer les instances représentatives du personnel de son rôle, organiser sa consultation avant la mise en œuvre de tout nouveau traitement?*
- Définir les rôles, responsabilités et interactions entre toutes les parties prenantes dans le domaine « Informatique et libertés ».
    - ♦ *Recommandations : définir les activités du CIL / DPO (tenir la liste des traitements et assurer son accessibilité, veiller en toute indépendance au respect de la loi, rendre compte de son action au responsable de traitement, etc.), séparer les rôles entre l'administrateur ayant accès aux données et celui ayant accès aux traces, décrire les interactions entre les maîtrises d'ouvrages, le responsable SSI et le CIL / DPO notamment dans le cadre de tout nouveau projet, définir les responsabilités spécifiques à la gestion des risques pesant sur les libertés et la vie privée, décrire la manière dont les violations de données à caractère personnel sont traitées.*
- Créer un comité de suivi, composé du responsable des traitements, de la personne en charge de l'assister dans la mise en application de la loi informatique et libertés / du RGPD et des parties intéressées, et se réunissant de manière régulière (au moins une fois par an) pour fixer des objectifs et faire un point sur l'ensemble des traitements de l'organisme.

Notes

- Désigner un CIL / DPO offre un vecteur de sécurité juridique (il permet de garantir la conformité de l'organisme à la loi informatique et libertés et au RGPD), un facteur de simplification des formalités administratives (exonération de l'obligation de déclaration préalable des traitements ordinaires et courants), un accès personnalisé aux services de la CNIL (extranet, formations, suivi personnalisé, etc.), la preuve d'un engagement éthique et citoyen et un outil de valorisation du patrimoine

informationnel (possibilité de céder, transmettre ou louer les fichiers détenus par l'organisme dans le respect de la loi informatique et libertés).

27 Politique (gestion des règles)

Objectifs : disposer d'une base documentaire formalisant les objectifs et les règles à appliquer dans le domaine « Informatique et libertés » (plan d'action, révision régulière de la politique « Informatique et libertés », etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Formaliser les éléments importants relatifs au domaine « Informatique et libertés » au sein d'une base documentaire qui constitue la politique « Informatique et libertés », dans une forme adaptée aux différents contenus (risques, grands principes à respecter, objectifs à atteindre, règles à appliquer, etc.) et aux différentes cibles de communication (usagers, service en charge de l'informatique, décideurs, etc.).
    - ♦ *Recommandations : des exigences dans un cahier des charges, une lettre au personnel exprimant l'engagement de la direction, une charte pour les usagers des moyens informatiques et de communication, une procédure pour l'intégration des questions « Informatique et libertés » dans les projets, etc.*
- Faire connaître la politique « Informatique et libertés » aux personnes qui doivent l'appliquer.
- Permettre aux personnes qui doivent appliquer la politique « Informatique et libertés » de demander formellement une dérogation en cas de difficulté de mise en œuvre , étudier chaque demande de dérogation en termes d'impact sur les risques, et le cas échéant, faire valider les dérogations acceptables par le responsable de traitement et faire évoluer la politique « Informatique et libertés » en conséquence.
- Établir un plan d'action pluriannuel et suivre sa mise en œuvre .
- Prévoir les dérogations aux règles de la politique « Informatique et libertés ».
- Prévoir de prendre en compte les difficultés rencontrées dans l'application de la politique « Informatique et libertés ».
- Vérifier la conformité aux règles de la politique « Informatique et libertés » et la mise en œuvre du plan d'action de manière régulière.
    - ♦ *Recommandations : vérifier cette conformité au moins une fois par an.*
- Réviser la politique « Informatique et libertés » de manière régulière.

Outillage / Pour aller plus loin

- Voir le principe « Élaborer une politique SSI » du référentiel général de sécurité (RGS).
- Voir le guide ANSSI PSSI.

28 Protection contre les sources de risques non humaines

Objectifs : réduire ou éviter les risques liés à des sources non humaines (phénomènes climatiques, incendie, dégât des eaux, accidents internes ou externes, animaux, etc.) qui pourraient affecter la sécurité des données à caractère personnel (mesures de prévention, détection, protection, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place des moyens de prévention, détection et protection contre l'incendie.
  - ♦ *Recommandations : ranger les locaux (retirer cartons, matériels inutilisés, substances inflammables, etc.), les équiper en nombre suffisant d'extincteurs adaptés au type de feu (extincteurs à poudre, à liquide ou à gaz), en systèmes de détection de fumée sous alarme, et en système de détection de chaleur sous alarme, remontant les alertes de manière centralisée (gardiennage local, prestations externalisée, etc.), mettre en place une extinction par gaz inerte ou extraction d'air dans les salles informatique.*
- Mettre en place des moyens de surveillance de la température.
  - ♦ *Recommandations : équiper les locaux de systèmes de climatisation sous alarme (en cas de dépassement du seuil de température), remontant les alertes de manière centralisée.*
- Mettre en place des moyens de surveillance et de secours de l'alimentation électrique.
  - ♦ *Recommandations : protéger les équipements informatiques et de téléphonie des variations et coupures d'électricité par un groupe électrogène ou par des onduleurs gérant l'arrêt normal ou le fonctionnement en continu, placés sous alarme (en cas de coupure) et remontant les alertes de manière centralisée.*
- Mettre en place des moyens de prévention des dégâts des eaux.
  - ♦ *Recommandations : surélever les équipements informatiques et de téléphonie d'au moins 15cm par rapport au niveau du sol pour les salles informatiques situées en rez-de-chaussée, les éloigner des installations d'eau qui risqueraient de se rompre (plomberie, climatiseur, radiateur, etc.).*
- S'assurer que les services essentiels (électricité, eau, climatisation, etc.) sont correctement dimensionnés pour les systèmes pris en charge.
- Préciser dans les contrats de maintenance des équipements de fonctionnement des services essentiels et de sécurité (extincteurs, climatisation, eau, détection de fumée et de chaleur, détection d'ouverture et d'effraction, groupe électrogène, etc.) un délai d'intervention adapté en cas de défaillance, et les contrôler au moins une fois par an.
- En cas de fortes exigences de disponibilité, connecter l'infrastructure de télécommunications par au moins deux accès différents et indépendants, et faire en sorte de pouvoir basculer de l'un à l'autre très rapidement. Si les besoins de disponibilité sont très élevés, le recours à un site de secours doit être envisagé.

Outillage / Pour aller plus loin

- Voir les référentiels du centre national de prévention et de protection, de l'assemblée plénière des sociétés d'assurances dommage et de la *National Fire Protection Association*.

29 Qualité des données : exactes et tenues à jour

Objectifs : être conforme à l'article 6 de la loi informatique et libertés et l'article 5.1(d) du règlement général sur la protection des données (RGPD) ; maintenir la qualité des données pour éviter des calculs à partir de données erronées ou obsolètes.

Bonnes pratiques

- Vérifier régulièrement l'exactitude des données personnelles de l'utilisateur.
- Inviter l'utilisateur à contrôler et, si nécessaire, mettre à jour ses données régulièrement.
- Assurer la traçabilité de toute modification des données.

Notes

- L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.

30 Recueil du consentement

30.1 Mesures génériques

Objectifs : être conforme à l'article 7 de la loi informatique et libertés et les articles 7 et 8 du règlement général sur la protection des données (RGPD) ; permettre un choix libre, spécifique et éclairé ; vérifier que le traitement ne repose pas sur une autre base légale que le consentement, tel que prévu à l'article 7 de la loi informatique et libertés et à l'article 6 du RGPD (obligation légale, sauvegarde de la vie, mission de service public, contrat ou mesures prises avec la personne, intérêt légitime).

Bonnes pratiques

• Déterminer et justifier les moyens pratiques qui vont être mis en œuvre pour obtenir le consentement des personnes concernées ou justifier de l'impossibilité de les mettre en œuvre :

- ♦ consentement exprès à l'inscription ;
- ♦ consentement segmenté par catégorie de données ou types de traitement ;
- ♦ consentement exprès avant le partage de données avec des tiers ;
- ♦ consentement présenté de manière compréhensible et adapté à la personne cible (notamment pour les enfants) ;
- ♦ recueil du consentement des parents pour les mineurs de moins de 13 ans ;
- ♦ pour une nouvelle personne, mise en œuvre d'un nouveau recueil de consentement ;
- ♦ après une longue période sans utilisation, demande à la personne concernée de réaffirmer son consentement ;
- ♦ si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface signale clairement que ce traitement a lieu (icône, voyant lumineux) ;
- ♦ si l'utilisateur change de contrat, les paramètres liés à son consentement sont maintenus.

- S'assurer que le traitement ne puisse pas être mis en œuvre sans consentement.
  - ♦ *Recommandations : étudier les cas où les moyens pratiques choisis ne sont plus opérationnels et déterminer des solutions de secours le cas échéant.*
- S'assurer que le consentement sera obtenu de manière libre.
  - ♦ *Recommandations : vérifier qu'il existe une alternative qui ne soit pas trop contraignante (un choix doit être possible) et qu'il n'y a pas de lien de subordination (par exemple entre un employé et son employeur).*
- S'assurer que le consentement sera obtenu de manière éclairée et transparente quant aux finalités du traitement.
- S'assurer que le consentement sera obtenu de manière spécifique à une finalité.

- En cas de sous-traitance, encadrer les obligations de chacun dans un document écrit, explicite et accepté des deux parties.
- Recueillir le consentement des parents pour les mineurs de moins de 13 ans.

Notes

- La CNIL considère que le consentement d'un salarié vis-à-vis d'un traitement mis en place par son employeur n'est pas libre, compte tenu du rapport de subordination.
- Les moyens pratiques permettant d'obtenir le consentement comprennent des actions que les personnes doivent réaliser (taper son code PIN - *Personal Identification Number* ou numéro d'identification personnel, approcher son téléphone mobile d'un panneau publicitaire dans le cas de l'envoi de publicités d'un panneau à un téléphone en Bluetooth, requérir d'approcher son périphérique NFC - *Near Field Communication o*u communication en champ proche, d'un lecteur?).
- Pour toute offre directe de services de la société de l'information à destination des mineurs, la charge de la preuve du consentement incombe au responsable de traitement (ou au sous-traitant), qui doit s'efforcer de vérifier que celui-ci est bien donné par le responsable parental (raisonnablement, compte tenu des moyens technologiques disponibles).

Outillage / Pour aller plus loin

- Voir l'article 32. II. de la loi informatique et libertés .
- Voir l'article L. 34-5 du Code des postes et communications électroniques sur les dispositions spécifiques à la prospection commerciale.

30.2 Spécificités pour les données relevant de l'article 8 de la loi informatique et libertés

Objectifs : permettre un choix libre, spécifique et éclairé, dans le cas de données relatives aux origines raciales ou ethniques, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale ou à la santé ou à la vie sexuelle des personnes.

Bonnes pratiques

• Obtenir le consentement éclairé et exprès des personnes concernées préalablement à la mise en œuvre du traitement, sauf dans le cas où le traitement repose sur une autre base légale ou que la loi prévoit qu'il est interdit de collecter ou de traiter ces données.

30.3 Spécificités pour la collecte de données via un site Internet

Bonnes pratiques

• Prévoir un formulaire avec des cases à cocher et qui ne sont pas cochées par défaut (dit « *opt-in* »).

30.4 Spécificités pour la collecte de données via des cookies

Bonnes pratiques

- Dans le cas où le cookie n'est pas strictement nécessaire à la fourniture du service expressément demandé par l'utilisateur, recueillir le consentement de l'internaute (ex :
  via une bannière en haut d'une page web
  (https://www.cnil.fr/fr/exemple-de-bandeau-cookie), une zone de demande de consentement en surimpression sur la page, des cases à cocher lors de l'inscription à un service en ligne, etc.) après information de celui-ci et avant le dépôt du cookie.
  - ♦ Recommandations : s'assurer que l'information est rédigée en termes simples et compréhensibles du grand public, tout en étant précise (ex : si le cookie a pour finalité de "créer des profils d'utilisateurs afin d'adresser des publicités ciblées", l'information devra reprendre l'ensemble de ces termes et non se limiter à indiquer "publicité").

Notes

- Pour qu'il y ait consentement libre et spécifique exprimé à travers les paramètres du navigateur, ce dernier doit pouvoir permettre à l'utilisateur de choisir quels cookies il accepte et pour quelle finalité. Un navigateur qui accepterait par principe tous les cookies sans distinguer leur finalité ne pourra pas être considéré comme permettant de donner un accord valable puisqu'il ne serait pas spécifique.

Outillage / Pour aller plus loin

- Voir les fiches pratiques https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite et
  https://www.cnil.fr/fr/recommandation-sur-les-cookies-quelles-obligations-pour-les-responsable sur le site de la CNIL.

30.5 Spécificités pour une collecte de données via un objet connecté ou une application mobile

Bonnes pratiques

- Recueillir le consentement de l'utilisateur au premier démarrage de l'objet ou de l'application mobile.

- ♦ *Recommandations : mettre en œuvre un nouveau recueil de consentement lors de la prise en main par un nouvel utilisateur ; après une longue période sans utilisation, demander à l'utilisateur de réaffirmer son consentement ; maintenir les paramètres liés au consentement en cas de changement d'appareil ou de réinstallation de l'application.*

- Proposer un consentement segmenté par catégorie de données ou types de traitement, en distinguant notamment le partage de données avec d'autres utilisateurs ou avec des sociétés tierces.
  - ♦ *Recommandations : si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface doit signaler clairement quand ce traitement a lieu (icône, voyant lumineux) ; laisser à l'utilisateur la possibilité d'accéder à tout moment aux réglages de son consentement.*

30.6 Spécificités pour la géolocalisation via un smartphone

Bonnes pratiques

- Permettre à l'usager de refuser qu'une application puisse le géolocaliser de manière systématique.
- Permettre à l'usager de sélectionner quelle application peut utiliser la géolocalisation.
- Permettre à l'usager de choisir quelles personnes peuvent accéder à l'information de géolocalisation le concernant et avec quelle précision.
-

30.7 Spécificités pour l'utilisation de techniques de publicité ciblée

Bonnes pratiques

• Mettre à disposition des utilisateurs des moyens simples et non payants pour accepter ou refuser la diffusion à leur égard de contenus publicitaires adaptés à leur comportement de navigation, et choisir les centres d'intérêts à propos desquels ils souhaiteraient voir s'afficher des offres publicitaires adaptées à leurs souhaits.

- ♦ *Recommandations : mettre une plateforme à disposition des internautes pour accepter ou refuser, totalement ou partiellement, l'affichage de publicités ciblées comportementales, expliquer comment supprimer les fichiers cookies et les historiques de navigation, choisir d'autoriser ou d'interdire le stockage de cookies, permettre de créer et stocker des cookies manifestant la volonté de ne pas faire l'objet de publicités comportementales de la part de tiers?*

30.8 Spécificités pour des recherches sur des prélèvements biologiques identifiants (i.e. l'ADN)

Bonnes pratiques

- Si les prélèvements sont conservés pour un traitement ultérieur différent du traitement initial, s'assurer également du consentement éclairé et exprès de la personne concernée pour cet autre traitement.

31 Relations avec les tiers

31.1 Mesures génériques

Objectifs : réduire les risques que les accès légitimes aux données par des tiers peuvent faire peser sur les libertés et la vie privée des personnes concernées (identification des tiers, contrat de sous-traitance, convention, BCR, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Identifier tous les tiers qui ont ou pourraient avoir un accès légitime aux données.
  - ♦ *Recommandations : certaines catégories de personnels, un prestataire en régie, la maintenance informatique, des partenaires métiers, les tiers autorisés.*
- Déterminer leur rôle vis-à-vis du traitement (administrateur informatique, sous-traitant, destinataire, personnes chargées de traiter les données, tiers autorisé) en fonction des actions qu'ils vont réaliser.
  - ♦ *Recommandations : en cas de recours à un fournisseur de service de cloud computing, celui-ci est généralement sous-traitant, bien qu'il puisse être considéré comme responsable de traitement dans certains cas.*
- Déterminer les responsabilités respectives en fonction des risques liés à ces données.
- Déterminer la forme appropriée pour fixer les droits et obligations selon la forme juridique des tiers et leur localisation géographique.
  - ♦ *Recommandations : un contrat de sous-traitance, une convention, un arrêté, des règles internes contraignantes (Binding Corporate Rules ? BCR).*
- Formaliser les règles que les personnes doivent respecter durant tout le cycle de vie de la relation liée au traitement ou aux données, selon la catégorie de personnes et les actions qu'elles vont réaliser.

Outillage / Pour aller plus loin

- Voir les notes CNIL Transfert Hors UE et CNIL Externaliser Hors UE pour le cas de transferts de données en dehors de l'Union européenne.

31.2 Spécificités pour les tiers prestataires de service travaillant dans les locaux de l'organisme

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques :

- Appliquer à ces prestataires les mêmes mesures que pour les salariés de l'organisme : formation aux enjeux Informatique et libertés, obligation de respecter les règles d'usage des ressources informatiques de l'organisme annexées au règlement intérieur.

- Fournir à ces prestataires un poste de travail interne à l'organisme ou s'assurer que l'utilisation du poste de travail fourni par leur employeur est compatible avec les objectifs de sécurité de l'organisme.
- S'assurer que ces prestataires sont bien engagés auprès de leur employeur par une clause de confidentialité applicable aux organismes clients de leur employeur.
- Gérer les habilitations de ces prestataires de façon spécifique en leur attribuant des habilitations limitées dans le temps prenant fin automatiquement à la date prévisionnelle de la fin de leur mission.
-

31.3 Spécificités pour les tiers destinataires

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Encadrer contractuellement la transmission des données à ces tiers, en précisant :
  - ♦ Les données transmises.
  - ♦ La ou les finalités pour lesquelles les personnes ont consenti à la transmission de leurs données au tiers (abonnement à une newsletter, prospection commerciale...).
  - ♦ Les modalités suivant lesquelles les personnes pourront exercer leurs droits.
  - ♦ Les mesures techniques mises en œuvre pour assurer la sécurité des données lors de leur transmission au tiers.
- Imposer au tiers de publier une politique de protection de la vie privée couvrant les traitements alimentés par les données transmises et précisant les objectifs de sécurité issus de la politique de sécurité des systèmes d'information.
- Si la transmission de données est faite via Internet toujours chiffrer les flux de données.
- Systématiquement informer le tiers lorsque des personnes exercent leur droit de rectification.

31.4 Spécificités pour les tiers autorisés

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Ne répondre qu'aux demandes transmises de façon formelle (courrier postal, fax) et répondre via le même canal de communication. Ne pas prendre en compte les demandes adressées par mail ni ne répondre par ce canal de communication.
- Vérifier la base légale de chaque demande de communication.
- Authentifier les émetteurs et ne répondre qu'à eux.
- Répondre de façon stricte à la demande en ne fournissant que les données mentionnées dans la demande.

32 Sauvegardes

Objectifs : assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité (régularité des sauvegardes, chiffrement du canal de transmission des données, test d'intégrité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effectuer une sauvegarde des données, qu'elles soient sous forme papier ou électronique, de manière régulière, selon les besoins de disponibilité et d'intégrité des métiers.
  - ♦ *Recommandations : une sauvegarde incrémentale peut être effectuée quotidiennement, une sauvegarde complète peut être effectuée avec une fréquence hebdomadaire et une copie des documents papiers peut être réalisée dès qu'ils sont édités ; la vérification des sauvegardes peut être effectuée automatiquement après celle-ci permettant de garantir l'intégrité par la production d'un rapport de fin de sauvegarde.*
- Mettre en œuvre des mécanismes de chiffrement du canal de transmission des données dans le cas où la sauvegarde est automatisée par le réseau.
- Protéger les données sauvegardées au même niveau de sécurité qu'en exploitation.
  - ♦ *Recommandations : les données sauvegardées sont déjà chiffrées, les sauvegardes sont chiffrées, ou le lieu de stockage des sauvegardes non chiffrées dispose d'un accès suffisamment protégé ; stocker les supports de sauvegardes physiques (bandes, cartouches, disques,etc.) dans des locaux différents de ceux où sont stockées les données traitées, et ce, dans une armoire ignifugée et étanche ; protéger le transport des supports de sauvegardes (transfert par agent habilité, transport dans un conteneur sécurisé, etc.).*
- Tester les sauvegardes de manière régulière.
  - ♦ *Recommandations : la récupération d'un échantillon de données peut être testée avec une fréquence mensuelle et la récupération de l'ensemble de données avec une fréquence annuelle.*
- Tester l'intégrité des données sauvegardées si les besoins des métiers le nécessitent.
  - ♦ *Recommandations : la fonction de hachage SHA-256 est utilisée pour réaliser une empreinte des données sauvegardée, voire une signature électronique, etc.*
- Formaliser le niveau d'engagement du service en charge de l'informatique vis-à-vis du recouvrement des informations chiffrées en cas de perte ou d'indisponibilité des secrets assurant le chiffrement (mots de passe, certificats?) et contrôler régulièrement les procédures en cohérence avec l'engagement pris.
- S'assurer que l'organisation, les personnels, systèmes et locaux nécessaires au traitement sont disponibles dans un délai correspondant aux besoins des métiers.
- S'assurer de la localisation géographique des sauvegardes, notamment vérifier dans quel(s) pays les données seront stockées.

Notes

- Les transferts, et donc les sauvegardes, de données vers des pays situés en-dehors de l'Union européenne sont interdits sauf :
  - ♦ si le transfert a lieu vers un pays reconnu comme « adéquat » par la Commission européenne ;
  - ♦ si des clauses contractuelles types, approuvées par la Commission européenne, sont signées entre l'émetteur et le destinataire des données ;
  - ♦ au sein d'un groupe, si des règles internes d'entreprises (BCR) sont adoptées ;
  - ♦ si dans le cas d'un transfert vers les États-Unis, l'entreprise destinataire a adhéré au Privacy Shield ;
  - ♦ si l'une des exceptions prévues par l'article 69 de la loi informatique et libertés est invoquée.
- Le site de la CNIL maintient une carte du monde indiquant les formalités à accomplir en fonction du pays visé. Dans tous les cas, le responsable du traitement reste responsable de la sécurité des données sauvegardées.
- La mise en place d'un plan et d'une procédure de sauvegarde doivent permettre d'assurer l'intégrité et la pérennité des données à caractère personnel, sans pour autant mettre en cause leur confidentialité. Le plan de sauvegarde doit mettre en évidence les objectifs généraux attendus des sauvegardes en matière de protection des données et déterminer les mesures organisationnelles nécessaires pour les atteindre. La procédure de sauvegarde détermine les moyens opérationnels et techniques qui doivent être mis en œuvre pour satisfaire au plan de sauvegarde.

33 Sous-traitance : identifiée et contractualisée

33.1 Mesures génériques

Objectifs : être conforme à l'article 28 du règlement général sur la protection des données (RGPD) ; encadrer la sous-traitance.

Bonnes pratiques

- Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'art. 28 du RGPD :
  - ♦ durée et périmètre de la sous-traitance,
  - ♦ finalité de la sous-traitance,
  - ♦ instructions de traitement documentées,
  - ♦ autorisation préalable en cas de recours à un autre sous-traitant,
  - ♦ mise à disposition de toute documentation apportant la preuve du respect du RGPD,
  - ♦ notification immédiate de toute violation de données, ♦ etc.

33.2 Spécificités pour les sous-traitants (hébergeur, mainteneur, administrateur, prestataires spécialisés...) hors fournisseurs de services de *cloud computing*

Bonnes pratiques

- Encadrer la relation de sous-traitance via un contrat conclu intuitu personæ.
- Exiger du sous-traitant la transmission de sa Politique de Sécurité des Systèmes d'Information (PSSI) ainsi que de toute les preuves de ses certifications en matière de sécurité de l'information et annexer ces documents au contrat. S'assurer que les mesures issues de sa PSSI sont conformes avec les recommandations de la CNIL en matière.
- Déterminer et fixer contractuellement de façon très précise les opérations que le sous-traitant sera amené à effectuer sur les données à caractère personnel :
  - ♦ Les données auxquelles il aura accès ou qui lui seront transmises.
  - ♦ les opérations qu'il doit réaliser sur les données.
  - ♦ La durée pendant laquelle il pourra conserver les données.
  - ♦ Les éventuels destinataires auxquels le responsable de traitement lui demande de transmettre les données.

- ♦ Les opérations à réaliser à la fin de la prestation (suppression définitive des données ou restitution des données dans le cadre d'une réversibilité puis destruction des données chez le sous-traitant).
- ♦ Les objectifs de sécurité fixés par le responsable de traitement.

- Déterminer contractuellement la répartition des responsabilité vis à vis des processus légaux visant à permettre l'exercice des droits des personnes.
- Interdire explicitement ou encadrer le recours à des sous-traitants de rang 2.
- Préciser dans le contrat que le respect des obligations Informatique et Libertés est une obligation essentielle du contrat.

33.3 Spécificités pour les fournisseurs de services de *cloud computing*

Bonnes pratiques

En plus des bonnes pratiques applicables en cas de recours à un sous-traitant, les mesures suivantes pourraient être mise en œuvre :

- Imposer au fournisseur une séparation a minima logique entre les données de l'organisme et les données de ses autres clients.
- Définir très précisément les lieux dans lesquels les données sont susceptibles d'être stockées, et les pays depuis lesquels les données stockées dans le *cloud* sont susceptibles d'être accessibles.
  - ♦ *Recommandation : les fournisseurs de services de cloud computing précisent souvent le lieux de stockage des données, mais n'indiquent que rarement les zones géographiques depuis lesquelles leur administrateurs accèdent à leur plateforme ; ce point doit être précisé dans le contrat.*
- Consulter la recommandation de la CNIL sur le *cloud computing*

34 Supervision

Objectifs : disposer d'une vision globale et à jour de l'état de protection des données et de la conformité à la loi informatique et libertés (contrôler la conformité des traitements, objectifs et indicateurs, responsabilités, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Effectuer régulièrement des contrôles des traitements de données afin de vérifier leur conformité à la loi informatique et libertés ainsi que l'effectivité et l'adéquation des mesures prévues.
  - ♦ *Recommandations : réaliser des vérifications sur les traitements les plus sensibles, sur ceux qui ont fait l'objet de violations de données ou de plaintes, et au hasard afin de tous les contrôler de manière récurrente ; faire réaliser un audit par une tierce partie de manière occasionnelle notamment sur les traitements les plus sensibles.*
- Fixer des objectifs dans le domaine « Informatique et libertés » et des indicateurs permettant de vérifier l'atteinte de ces objectifs.
  - ♦ *Recommandations : disposer d'une cartographie des traitements de données et des risques associés, réaliser les formalités préalables auprès de la CNIL pour l'ensemble des traitements et ce, avant leur mise en œuvre opérationnelle.*
- Déterminer les responsabilités respectives en fonction des risques liés à ces données.
  - ♦ *Recommandations : faire un « RACI », c'est-à-dire déterminer qui réalise chaque action (R pour « Responsible »), qui en est responsable (A pour « Accountable »), qui participe (C pour « Consulted ») et qui doit en être informé (I pour « Informed »).*
- Faire un bilan « Informatique et libertés » de manière régulière.
  - ♦ *Recommandations : présenter de manière annuelle une cartographie globale des risques pesant sur tous les traitements à leur responsable, une évaluation de la conformité à la politique « Informatique et libertés », un avancement des actions prévues.*

Outillage / Pour aller plus loin

- La CNIL labellise des procédures d'audit « Informatique et libertés ».
- Afin de connaître les formalités préalablement réalisées auprès de la CNIL par son organisme, il est possible de demander à la CNIL une « liste article 31 » par télécopie au 01 53 73 22 00, en précisant le numéro de SIREN et les coordonnées de l'organisme.
- Voir le guide d'élaboration de tableaux de bord de sécurité des systèmes d'information (TDBSSI) mis en ligne par l'ANSSI.

35 Surveillance

35.1 Mesures génériques

Objectifs : être capable de détecter les incidents concernant des données à caractère personnel de façon précoce, et de disposer d'éléments exploitables pour les étudier ou pour fournir des preuves dans le cadre d'enquêtes (architecture et politique de journalisation, respect des obligation en matière de protection des données à caractère personnel, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une architecture de journalisation permettant de conserver une trace des événements de sécurité et du moment où ils ont eu lieu.
    - ♦ *Recommandations : horodater les événements journalismes en prenant comme référence le temps UTC (Coordinated Universal Time), utiliser une source de temps fiable sur laquelle les équipements se synchroniseront, telle qu'un serveur NTP (Network Time Protocol) ou une radiosynchronisation, centraliser localement (regrouper tous les journaux sur une machine de collecte relativement isolée et accompagnée d'un poste de travail de consultation dédié), exporter les journaux (envois planifiés, transfert automatique ou utilisation d'un réseau d'administration), disposer d'une capacité de stockage suffisante, se doter d'un système d'archivage et de sauvegarde pour les journaux d'événements, protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés, etc.*
- Choisir les événements à journaliser en fonction du contexte, des supports (postes de travail, pare-feu, équipements réseau, serveurs, etc.), des risques et du cadre légal.
    - ♦ *Recommandations : journaliser les actions sur les postes de travail en cas de risques élevés uniquement, respecter le code des postes et des communications électroniques en cas de mise en place d'un accès public à Internet (conserver pendant un an les données de connexion si elles sont collectées dans le cadre du service, les informations permettant d'identifier l'utilisateur ainsi que le ou les destinataires de la communication, données relatives aux équipements terminaux de communication utilisés, caractéristiques techniques, la date, l'horaire et la durée de chaque communication, et les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs), avec un devoir strict de confidentialité, respecter le décret LCEN (Loi pour la confiance dans l'économie numérique) en cas de création de contenu en ligne (conserver pendant un an, si elles sont collectées dans le cadre du service : données de connexion, données de création de contenu, données relatives au contrat, données relatives au paiement), etc.*
- Respecter les exigences de la loi informatique et libertés si les événements journalisés comprennent des données à caractère personnel.

- ♦ *Recommandations : les dispositifs utilisés doivent faire l'objet d'une information des utilisateurs, d'une déclaration à la CNIL, l'utilisation des données collectées doit respecter la finalité initialement déclarée, etc.*

- Procéder périodiquement à l'analyse des informations journalisées, voire mettre en place un système de détection automatique de signaux faibles.
- Conserver les journaux d'événements sur six mois, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Outillage / Pour aller plus loin

- Voir la note CERTA Journaux.
- En fonction de l'étude des risques et des contraintes légales, la fonction "Horodatage" du référentiel général de sécurité (RGS) est à considérer.

35.2 Spécificités pour un poste client

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- S'assurer que la taille maximale des journaux d'événements est suffisante, et notamment que les événements les plus anciens ne sont pas supprimés automatiquement si la taille maximale est atteinte.
- Journaliser les événements relatifs aux applications, à la sécurité et au système.
  - ♦ *Recommandations : connexions au système (enregistrer l'identifiant, la date et l'heure de leur tentative de connexion, le fait que la connexion ait réussi ou non, ainsi que la date et l'heure de la déconnexion), modification de paramètres de sécurité, de privilèges, de comptes utilisateurs et de groupes, événements système (arrêt / redémarrage de processus système sensibles), accès/modification de données système, échec lors d'un accès à une ressource (fichier système, objet, réseau, etc.), exécution de transactions sensibles, l'application des correctifs de sécurité, actions d'administration et de prise de main à distance, journaux du logiciel antivirus (activation/désactivation, mises à jour, détection de codes malveillants), etc.*
- Exporter les journaux à l'aide des fonctionnalités de gestion du domaine ou via un client *syslog*.
- Analyser principalement les heures de connexions et déconnexions, le type de protocole utilisé pour se connecter et le type d'utilisateur qui y a recours, l'adresse IP d'origine de la connexion, les échecs successifs de connexions, les arrêts inopinés d'applications ou de tâches.

35.3 Spécificités pour un pare-feu

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une politique de filtrage interdisant toute communication directe entre des postes internes et l'extérieur (ne permettre les connexions que via le pare-feu) et ne laisser passer que les flux explicitement autorisés (blocage par le pare-feu de toute connexion sauf celles identifiées comme nécessaires).
- Journaliser toutes les connexions autorisées réussies et toutes les tentatives de connexions rejetées.
    - ♦ *Recommandations : pour chaque connexion, horodater les journaux à la milliseconde près, journaliser au moins les adresses IP source et destination, le protocole de transport, et les drapeaux et états de connexion associés aux segments pour le protocole TCP, etc.*
- Exporter les journaux par un canal sécurisé vers un serveur dédié.

35.4 Spécificités pour un équipement réseau

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Journaliser l'activité sur chaque port d'un commutateur ou d'un routeur.
- Exporter les journaux vers un serveur dédié à l'aide d'un client *syslog* intégré ou via un flux *netflow*.
- Contrôler la volumétrie en fonction des heures, ainsi que le respect des éventuelles listes de contrôle d'accès (ACL : *Access Control Lists*) pour les routeurs.

35.5 Spécificités pour un serveur

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Journaliser le maximum d'informations sur les requêtes effectuées par les clients sur les serveurs web dans le but d'identifier les défauts de configuration, les injections de requêtes SQL, etc.
    - ♦ *Recommandations : connexions réussies, méthodes de connexion, requêtes effectuées, volumétries, répartition par pays des requêtes, etc.*
- Journaliser l'activité des usagers sur les serveurs *proxy*.
- Journaliser l'ensemble des requêtes qui sont faites aux serveurs DNS, qu'elles soient émises par des internautes ou par des clients du réseau interne.
- Journaliser les données d'authentification horodatées et la durée de chaque connexion sur les serveurs d'accès distant.
- Journaliser la réception et la gestion des messages sur les serveurs de messagerie.

36 Sécurité de l'exploitation

Objectifs : limiter la vraisemblance et la gravité des risques visant les biens supports utilisés en exploitation (documenter les procédures d'exploitation, inventaire et mise à jour des logiciels et matériels, correction des vulnérabilités, duplication des données, limiter l'accès physique au matériel, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Documenter les procédures d'exploitation, les tenir à jour et les communiquer à tous les utilisateurs concernés (toute action sur le système, qu'il s'agisse d'opérations d'administration ou de la simple utilisation d'une application, doit être expliquée dans des documents auxquels les utilisateurs peuvent se référer).
- Tenir à jour un inventaire des logiciels et matériels utilisés en exploitation.
    - ♦ *Recommandations : maintenir une liste exhaustive des logiciels, des serveurs physiques et virtuels, des éléments d'infrastructures, des services gérés par des tiers et des équipements réseaux et de télécommunications utilisés pour l'exploitation des traitements de données personnelles. Inclure dans cette liste les informations matérielles, les types de système d'exploitation, les informations réseau (adresse IP, adresse MAC), les applications utilisées, les versions présentes et les correctifs appliqués, et les versions des firmwares pour les équipements pour lesquels ceux-ci peuvent être mis à jour).*
- Réaliser une veille sur vulnérabilités découvertes dans les logiciels (y compris les firmwares) utilisés en exploitation, et les corriger dès que possible.
    - ♦ *Recommandations : dans la mesure du possible activer les systèmes de mise à jour automatique des logiciels. Lorsque cela n'est pas possible, installer les mises à jour correctives dès leur disponibilité. A défaut mettre en place des mécanismes visant à prévenir l'exploitation des vulnérabilités découvertes.*
- Formaliser les procédures de mises à jour matérielles et logicielles.
- Interdire l'usage des serveurs de production (serveurs de base de données, serveur web, serveur de messagerie, etc.) pour d'autres fins que celles prévues initialement
    - ♦ *Recommandations : n'installer que les logiciels strictement nécessaires sur les serveurs, limiter le trafic réseau aux ports strictement nécessaires.*
- Utiliser des unités de stockage de données utilisant des mécanismes de redondance matérielle (tel que le RAID), ou bien des mécanismes de duplication des données entre plusieurs serveurs et/ou sites.
- Vérifier que le dimensionnement des capacités de stockage et de calcul est suffisant pour assurer le fonctionnement correct des traitements, même en cas de pic d'activité.
- Vérifier que les conditions physiques d'hébergement (température, humidité, fourniture d'énergie, etc.) sont appropriés à l'usage prévu des matériels, et incluent des mécanismes de secours (onduleur et/ou alimentation de secours et/ou groupe électrogène).

- Limiter l'accès physique aux matériels sensibles et/ou qui ont une grande valeur marchande.
- Limiter les possibilités de modification des matériels
    - ♦ *Recommandations : utiliser des scellés permettant de vérifier qu'un ordinateur a été ouvert, cadenasser les boîtiers des machines lorsque cela est possible, verrouiller les baies de stockage.*
- Prévoir un Plan de Reprise d'Activité (PRA) ou un Plan de Continuité d'Activité (PCA), en fonction des objectifs de disponibilité des traitements mis en œuvre .
    - ♦ *Recommandations : formaliser le PRA ou le PCA, le diffuser auprès des personnels concernés (internes, externes, prestataires), tester régulièrement son efficacité.*
- Mettre en place une procédure de gestion des incidents de sécurité permettant de les détecter, les enregistrer, les qualifier et les traiter (voir la page Gestion des incidents et des violations de données).

37 Sécurité des canaux informatiques (réseaux)

37.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des canaux informatiques (réseau filaire, wifi, ondes radio, fibre optique, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (cartographie du réseau, pare-feu, détection et prévention d'intrusion, protocole SSH, chiffrement des flux, authentification forte, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Maintenir à jour une cartographie détaillée du réseau.
- Recenser tous les accès Internet, les intégrer dans la cartographie du réseau et s'assurer que les mesures prévues sont bien appliquées à chacun d'entre eux.
- Assurer la disponibilité des canaux informatiques.
    - ♦ *Recommandations : vérifier que les canaux informatiques sont correctement dimensionnés par rapport aux flux prévus, prévoir des solutions alternatives en cas de dysfonctionnement.*
- Segmenter le réseau en sous-réseaux logiques étanches selon les services censés y être déployés.
    - ♦ *Recommandations : cloisonner les réseaux dans des réseaux virtuels (VLAN) pour regrouper certains matériels selon des critères logiques, ou éventuellement en contrôlant les flux de données sur la base des adresses réseau en mettant en place des réseaux physiques distincts, dans le but de séparer les trafics réseau entre les différents groupes ainsi constitués.*
- Interdire toute communication directe entre des postes internes et l'extérieur.
    - ♦ *Recommandations : différencier un réseau interne pour lequel aucune connexion venant d'Internet n'est autorisée, et un réseau dit DMZ accessible depuis Internet.*
- N'utiliser que les flux explicitement autorisés (limiter les ports de communication strictement nécessaires au bon fonctionnement des applications installées) à l'aide d'un pare-feu.
    - ♦ *Recommandations : si l'accès à un serveur web passe obligatoirement et uniquement par l'utilisation du protocole SSL, il faut autoriser uniquement les flux réseau IP entrants sur cette machine sur le port de communication 443 et bloquer tous les autres ports de communication, etc.*
- Surveiller l'activité réseau après en avoir informé les personnes concernées.
    - ♦ *Recommandations : mettre en place des systèmes de détection d'intrusion ou un système de prévention d'intrusion en vue d'analyser le trafic réseau en temps réel pour détecter toute activité suspecte évoquant un scénario d'attaque informatique.*
- Prévoir un plan de réponse en cas d'intrusion majeure contenant les mesures organisationnelles et techniques pour délimiter et circonscrire la compromission.

- ♦ *Recommandations : préparation des documents nécessaires à la gestion de crise (cartographie du réseau, liste des personnels en mesure d'intervenir sur les systèmes, coordonnées des administrations ou organisations susceptibles de porter assistance, etc.).*

- Identifier les matériels de manière automatique comme moyen d'authentification des connexions à partir de lieux et matériels spécifiques.
  - ♦ *Recommandations : utiliser les identifiants uniques des cartes réseau (l'adresse MAC) afin de détecter et d'empêcher la connexion d'un dispositif non répertorié.*
- Sécuriser les flux d'administration et restreindre, voire interdire, l'accès physique et logique aux ports de diagnostic et de configuration à distance.
  - ♦ *Recommandations : les opérations d'administration sur les ressources locales doivent s'appuyer sur des protocoles d'administration sécurisés, et dans le cas où le recours à de tels protocoles est techniquement impossible, l'administration doit être accomplie directement sur l'équipement concerné, restreindre l'usage du protocole SNMP qui permet la configuration des équipements réseau par connexion sur les ports UDP 161 et 162.*
- Interdire le raccordement d'équipements informatiques non maîtrisés.
  - ♦ *Recommandations : seuls les équipements (ordinateurs, assistants personnels, smartphones, etc.) dont la configuration a été expressément validée par le service en charge de l'informatique peuvent être raccordés ou synchronisés au réseau ou aux postes de travail.*
- Transmettre les secrets garantissant la confidentialité de données (clé de déchiffrement, mot de passe, etc.) dans une transmission distincte, si possible via un canal de nature différente de celui ayant servi à la transmission des données.
  - ♦ *Recommandations : envoyer un fichier chiffré par mail et communiquer le mot de passe par téléphone ou SMS.*

Outillage / Pour aller plus loin

- La surveillance de l'activité du réseau peut être réalisée à l'aide :
  - ♦ de systèmes de détection d'intrusions ou IDS (soit des NIDS qui surveillent l'état de la sécurité au niveau du réseau, soit des HIDS qui surveillent l'état de la sécurité au niveau des ordinateurs reliés au réseau, soit des IDS hybrides),
  - ♦ de système de prévention d'intrusion ou IPS (soit des NIPS qui détectent les flux réseau suspects au niveau des protocoles, soit des WIPS qui détectent les flux réseau sans fil suspects au niveau des protocoles, soit des NBA qui identifient les menaces générant des flux inhabituels, soit des HIPS qui surveillent des événements inhabituels au niveau des machines).
- Voir les notes CERTA Filtrage, CERTA SSL, CERTA Canulars, CERTA Spam, CERTA Tunnels, CERTA Indexation, CERTA PHP, CERTA IPv6, CERTA DNS et CERTA Backscatting.
- Voir les exigences relatives à la fonction « Authentification » du référentiel général de sécurité (RGS).

37.2 Spécificités pour les connexions aux équipements actifs du réseau

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

• Utiliser le protocole SSH ou une connexion directe à l'équipement pour la connexion aux équipements actifs du réseau (pare-feu, routeurs, commutateurs) et proscrire l'utilisation du protocole Telnet sauf en cas de connexion directe.

37.3 Spécificités pour les outils de prise de main à distance

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Limiter la prise de main à distance d'une ressource informatique locale aux agents du service en charge de l'informatique, sur les ressources informatiques de leur périmètre.
- Identifier les utilisateurs de l'outil de prise de main à distance de manière unique.
- Authentifier les utilisateurs de l'outil de prise de main à distance au moins par un mot de passe robuste et si possible par certificat électronique.
- Journaliser les actions des utilisateurs de l'outil de prise en main à distance (voir la page Traçabilité (journalisation)).
- Sécuriser le flux d'authentification sécurisé.
    - ♦ *Recommandations : aucun mot de passe en clair, séquence non rejouable.*
- La prise de main à distance doit être soumise à un accord préalable de l'utilisateur.
    - ♦ *Recommandations : validation sur une fenêtre pop-up.*
- Interdire la modification du paramétrage de sécurité de l'outil et la visualisation des mots de passe ou secrets utilisés.
- Empêcher la récupération des secrets utilisés pour établir la connexion à partir d'un poste de travail.
- Chiffrer l'ensemble des flux échangés.
- L'utilisateur doit être informé qu'une prise de main à distance est en cours sur son poste de travail (par exemple à l'aide d'une icône).

37.4 Spécificités pour les postes nomades ou se connectant à distance

Objectifs : réduire les risques liés à l'utilisation distante des postes nomades (PC portables, assistants personnels, etc.) ou se connectant à distance.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place une solution d'authentification forte des utilisateurs accédant à distance au système d'information interne (quand cela est possible).
    - ♦ *Recommandations : requérir au minimum deux éléments d'authentification distincts parmi ce que l'on sait (ex. : mot de passe, boitier électronique générateur de mots de passe à usage unique OTP (token) sans oublier de*

changer les mots de passe d'activation par défaut), ce que l'on a (ex. : certificat électronique, carte à puce, etc.) et une caractéristique qui nous est propre (ex. :
empreinte digitale, autre caractéristique biométrique).

- Chiffrer les communications entre le poste nomade et le système d'information interne.
  - ♦ *Recommandations : utiliser des lignes privées dédiées, mettre en place des connexions VPN reposant sur des algorithmes cryptographiques réputés forts, recourir au chiffrement de la communication par l'usage du protocole SSL avec une clé de 128 bits lors de la mise en œuvre de services web.*
- Installer un pare-feu local pour sécuriser les échanges réseau entrant et sortant sur le poste de travail en situation de nomadisme, qui doit être activé dès que le poste nomade sort de l'organisme.
  - ♦ *Recommandations : connecter le poste de travail sur une infrastructure d'accès distant spécifique, interdire les connexions simultanées au système d'information interne et à un réseau sans fil, interdire la possibilité de désactiver le pare-feu ou de modifier ses paramètres par les utilisateurs.*

37.5 Spécificités pour les interfaces sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Dans le cas de connexions à l'aide d'interfaces sans fil, interdire les communications non sécurisées.
- Interdire la connexion simultanée à un réseau via une interface sans fil et par l'interface Ethernet.
- Désactiver les interfaces de connexion sans fil (Wifi, Bluetooth, infrarouge, 4G, etc.) dès lors qu'elles ne sont pas utilisées, de manière matérielle ou logicielle.
- Maîtriser les réseaux sans fil.
  - ♦ *Recommandations : n'autoriser que la mise en place d'infrastructures sans fil permettant l'accès à des ressources locales par les collaborateurs (extension du réseau local) et d'accès publics à Internet totalement isolés de l'infrastructure réseau locale de l'organisme, authentifier les utilisateurs, chiffrer les flux.*

37.6 Spécificités pour le Wifi

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole WPA ou WPA2 avec un mode de chiffrement AES/CCMP ou, le mode « Enterprise » des protocoles WPA et WPA2 (utilisant un serveur Radius, ainsi que les sous-protocoles EAP-TLS ou PEAP).

- Interdire les réseaux ad-hoc.
- Utiliser et configurer un pare-feu au point d'entrée/sortie du réseau, afin de cloisonner les équipements connectés en fonction des besoins.

Outillage / Pour aller plus loin

- Voir la note CERTA Wifi.
- Voir le guide pratique spécifique pour la mise en place d'un accès Wifi de l'ASIP
- Dans certains contextes, le filtrage par adresse MAC peut être mis en place pour protéger l'accès Wifi.

37.7 Spécificités pour le Bluetooth

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Imposer une authentification mutuelle avec l'appareil distant.
- Limiter l'utilisation à l'échange de fichiers avec des matériels maîtrisés par le service en charge de l'informatique.
- Chiffrer les échanges.

Outillage / Pour aller plus loin

- Voir la note CERTA Bluetooth.

37.8 Spécificités pour l'infrarouge

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Réaliser une authentification avant la connexion, l'émission et la réception d'un fichier ou d'une commande.

37.9 Spécificités pour les réseaux de téléphonie mobile (2G, 3G ou 4G, etc.)

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Protéger la carte SIM par un code PIN demandé à chaque utilisation.

37.10 Spécificités pour la navigation sur Internet

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole TLS (HTTPS) pour assurer l'authentification des serveurs et la confidentialité des communications.
- Privilégier des clés générées conformément au RGS.
    - ♦ *Recommandations : avoir recours à un prestataire de service de certification électronique référencé comme conforme au RGS dans sa version 1.0 pour un usage d'authentification de serveur.*

37.11 Spécificités pour le transfert de fichiers

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Utiliser le protocole SFTP ou éventuellement le protocole SCP.
- Chiffrer les fichiers avant tout transfert dans le cas de risques élevés.

37.12 Spécificités pour le fax

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Positionner le fax dans un local physiquement contrôlé et accessible uniquement au personnel habilité.
- Mettre en place un contrôle par code d'accès personnel pour l'impression des messages.
- Faire afficher l'identité du fax destinataire lors de l'émission des messages, afin d'être assuré de l'identité du destinataire.
- Doubler l'envoi par fax d'un envoi des documents originaux au destinataire.
- Préenregistrer dans le carnet d'adresse des fax (si cette fonctionnalité existe) les destinataires potentiels.

37.13 Spécificités pour l'ADSL/Fibre

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Recenser les points d'accès locaux à Internet.
- Isoler physiquement les points d'accès locaux à Internet du réseau interne.
- Ne les utiliser qu'en cas de besoins spécifiques et justifiés (exemple : perte de disponibilité de l'accès au réseau inter-urbain).
- Ne les activer que lors de leur utilisation.
- Désactiver leur éventuelle interface sans fil (« wifi »).

37.14 Spécificités pour la messagerie électronique

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les pièces jointes contenant des données.
- Sensibiliser les utilisateurs au fait qu'ils doivent éviter d'ouvrir des courriers électroniques d'origine inconnue et encore plus les pièces jointes à risque (extensions .pif, .com, .bat, .exe, .vbs, .lnk, etc.) ou configurer le système de telle sorte qu'il ne soit pas possible de les ouvrir.
- Sensibiliser les utilisateurs au fait qu'il convient de ne pas relayer les canulars.

Outillage / Pour aller plus loin

- Définir une politique de gestion de l'authentification des courriers électroniques et recourir au protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance*) pour réduire leur usage abusif.

37.15 Spécificités pour les messageries instantanées

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Sensibiliser les utilisateurs.
  - ♦ *Recommandations : demander aux utilisateurs de faire attention à ce qu'ils écrivent, d'éviter de donner des vraies données dans les formulaires d'information sur les utilisateurs, de ne pas faire confiance aux pièces jointes (ne pas lancer des fichiers provenant d'inconnus), de ne pas suivre tous les liens hypertextes.*
- Interdire l'installation et l'utilisation de logiciels de messagerie instantanée, et si cela est néanmoins nécessaire, sensibiliser les utilisateurs aux risques et bonnes pratiques à adopter.
  - ♦ *Recommandations : leur demander de n'installer que les logiciels téléchargés depuis le site de l'éditeur.*

Outillage / Pour aller plus loin

- Voir la note CERTA IRC.

38 Sécurité des documents papier

Objectifs : limiter les risques que des personnes non autorisées accèdent aux documents papiers contenant des données à caractère personnel (mention de classification, procédés d'impression, limitation de la diffusion, traçage des transmissions, etc.).

38.1 Marquer les documents contenant des données

Objectifs : susciter une conduite prudente des personnes ayant accès aux documents en identifiant clairement ceux qui contiennent des données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Porter une mention visible et explicite sur chaque page des documents contenant des données sensibles.
  - ♦ *Recommandations : ajouter en en-tête ou en pied de page des modèles de documents utilisés dans le cadre du traitement la mention « Données à caractère personnel sensibles », voire « Ce document contient des données à caractère personnel, protégées par la Loi ».*
  - ♦ *Recommandations : ajouter « [Données à caractère personnel] » dans le titre des courriels en contenant au cas où ces derniers soient imprimés.*
- Porter une mention visible et explicite dans les applications métiers permettant d'accéder à des données et permettant de les imprimer.
  - ♦ *Recommandations : ajouter en en-tête ou en pied de page de l'application la mention « Cette application permet d'accéder à des données à caractère personnel, protégées par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la 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 », afficher une mention dans les courriers auxquels sont joints des données rappelant à l'expéditeur qu'il manipule des données qui ne doivent être transmises qu'aux destinataires prévus initialement et qui doivent être détruites à l'issue de la durée de conservation prévue.*

Notes

- Bien que des mentions visibles puissent attirer l'attention de personnes malveillantes, le gain escompté surpasse généralement le risque induit. En effet, une mention dans des courriers auxquels sont joints des fichiers contenant des données permet d'améliorer l'attention des expéditeurs et des destinataires, qui seront ainsi plus prudents en les manipulant. En outre, il sera plus aisé d'identifier des documents ou des courriers marqués afin de les détruire en fin de durée de conservation.

38.2 Réduire les vulnérabilités des documents papier

Objectifs : diminuer la possibilité que les caractéristiques des documents papier ne soient exploitées pour porter atteinte aux données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Choisir des supports papier et des procédés d'impression appropriés aux conditions de conservation (selon la durée de conservation, l'humidité ambiante, etc.).
- Récupérer les documents imprimés contenant des données immédiatement après leur impression ou effectuer, lorsque c'est possible, une impression sécurisé.
- Limiter la diffusion des documents papier contenant des données qu'aux personnes ayant le besoin d'en disposer dans le cadre de leur activité.
- Stocker les documents papier contenant des données dans un meuble sécurisé.
  - ♦ *Recommandations : utiliser une armoire ignifugée fermant à clé, un coffre, etc.*
- Détruire les documents papier contenant des données et qui ne sont plus utiles à l'aide d'un broyeur approprié.
  - ♦ *Recommandations : utiliser un broyeur certifié au minimum classe 3 de la norme DIN 32757105 (La norme allemande DIN 32757 définit 5 niveaux de sécurité pour les broyeurs selon la sensibilité des documents).*

Outillage / Pour aller plus loin

- Pour les documents les plus sensibles, il est conseillé d'en faire une copie et de les stocker de manière sécurisée et dans un lieu différent. Il est aussi possible de les placer sous scellé afin de détecter le fait que quelqu'un y ait accédé.

38.3 Réduire les vulnérabilités des canaux papier

Objectifs : diminuer la possibilité que les caractéristiques des canaux papier (circulation au sein de l'organisme, transport en véhicule, envoi par la Poste?) ne soient exploitées pour porter atteinte aux données à caractère personnel.

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- N'envoyer que les documents papier contenant des données nécessaires au traitement.
- Garder une trace précise de la transmission des documents papier contenant des données.
  - ♦ *Recommandations : noter sur un document prévu à cet effet une trace de l'envoi (liste des documents envoyés, identité de l'expéditeur et sa signature, canal de transmission, identité du transporteur le cas échéant et sa signature, date et heure d'envoi) et de la réception de documents contenant des données (liste des documents reçus, identité du destinataire et sa signature, date et heure de réception), etc.*

- Choisir un canal de transmission adapté aux risques et à la fréquence de transmission. ♦ *Recommandations : envoi par la Poste, emploi des ressources de l'organisme (véhicules et chauffeurs), recours à une entreprise spécialisée, etc.*
- Améliorer la confiance envers le transporteur de documents papier contenant des données.
    - ♦ *Recommandations : sensibiliser les personnes transportant les documents papier aux risques s'ils appartiennent à l'organisme, prévoir des clauses relatives à la protection de la disponibilité, de l'intégrité et de la confidentialité des documents papier dans le contrat établi avec un transporteur tiers, contrôler l'identité du transporteur, etc.*
- Protéger les documents papier contenant des données.
    - ♦ *Recommandations : envoyer les documents sous double enveloppe en recommandé, apposer une marque « Confidentiel » sur les enveloppes, prévoir des enveloppes, boîtes ou autres contenants plus ou moins sécurisés contre les menaces de nature non humaine (accidents, incendie, etc.), etc.*

Outillage / Pour aller plus loin

- Si les risques sont importants, il peut également être utile de conserver une copie des documents transmis, de prévoir la réaction en cas de vol, disparition ou modification sous la forme d'une procédure, et de placer les documents sous scellé afin de détecter les éventuellement compromissions.

39 Sécurité des matériels

39.1 Mesures génériques

Objectifs : diminuer la possibilité que les caractéristiques des matériels (serveurs, postes fixes, ordinateurs portables, périphériques, relais de communication, supports amovibles, etc.) soient exploitées pour porter atteinte aux données à caractère personnel (inventaire, cloisonnement, redondance matérielle, limiter l'accès, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Tenir à jour un inventaire des ressources informatiques utilisées.
  - ♦ *Recommandations : maintenir la liste des postes de travail et utilisateurs, des serveurs gérés localement, des équipements réseaux et de télécommunications et des autres périphériques (imprimantes, fax, etc.) en précisant les informations matérielles, le type de système d'exploitation, les informations réseau (adresse IP, adresse MAC), les principales applications portées, les versions présentes et correctifs appliqués.*
- Cloisonner les ressources de l'organisme en cas de partage de locaux.
  - ♦ *Recommandations : le réseau local utilisé par les collaborateurs doit s'appuyer sur des ressources réseau dédiées, isolées des ressources utilisées par les autres utilisateurs des locaux, et placées sous la responsabilité du service en charge de l'informatique ; en cas de partage des locaux techniques, l'accès aux ressources informatiques de l'organisme doit être restreint au service en charge de l'informatique (ex.: serveur dédié dans une baie fermée à clé).*
- Empêcher l'accès à des données stockées sur des ressources informatiques mises au rebut.
  - ♦ *Recommandations : inspecter l'équipement pour s'assurer que toute donnée a bien été effacée, entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès verbal de destruction des supports et le conserver pendant 10 ans.*
- Prévoir une redondance matérielle des unités de stockage par une technologie RAID ou équivalente.
- Vérifier que le dimensionnement des capacités de stockage et de traitement, ainsi que les conditions d'utilisation, sont appropriés à l'usage prévu des matériels, notamment en terme de place, d'humidité et de température.
- Vérifier que l'alimentation des matériels les plus critiques est protégée contre les variations de tension et qu'elle est secourue, ou qu'elle permet au moins de les arrêter normalement.
- Limiter l'accès aux matériels sensibles et/ou qui ont une grande valeur marchande.

- Limiter les possibilités de modification des matériels
    - ♦ *Recommandations : utiliser des scellés permettant de vérifier qu'un ordinateur a été ouvert, cadenasser les boîtiers des machines lorsque cela est possible, verrouiller les baies de stockage.*

39.2 Spécificités pour les postes de travail

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Assurer la mise à disposition et le maintien en conditions opérationnelles et de sécurité des postes de travail des utilisateurs par le service en charge de l'informatique.
- Protéger les postes peu volumineux, donc susceptibles d'être facilement emportés, et notamment les ordinateurs portables, à l'aide d'un câble physique de sécurité, dès que l'utilisateur ne se trouve pas à proximité et que le local n'est pas sécurisé physiquement.
- Récupérer les données, à l'exception des données signalées comme étant privées ou personnelles, présentes sur un poste préalablement à sa réaffectation à une autre personne.
- Effacer les données présentes sur un poste préalablement à sa réaffectation à une autre personne ou pour les postes partagés.
- Supprimer les données temporaires à chaque reconnexion des postes partagés.
- En cas de compromission d'un poste, rechercher toute trace d'intrusion dans le système afin de détecter si l'attaquant a compromis d'autres éléments.
-

39.3 Spécificités pour les postes nomades

Objectifs : réduire les risques liés au format, au caractère attractif et à l'utilisation des postes nomades (PC portables, assistants personnels, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Chiffrer les données stockées sur les postes nomades en respectant les mesures préconisées sur la page Chiffrement.
    - ♦ *Recommandations : chiffrement du disque dur dans sa totalité au niveau matériel, chiffrement du disque dur dans sa totalité à un niveau logique via le système d'exploitation ou un autre logiciel, chiffrement fichier par fichier, création de conteneurs chiffrés, etc.*
- Limiter le stockage de données sur les postes nomades au strict nécessaire, et éventuellement l'interdire lors des déplacements à l'étranger.
- Assurer la disponibilité des données stockées sur les postes nomades.
    - ♦ *Recommandations : les copier dès que possible sur un autre poste, sur un serveur, etc.*

- Purger les données collectées sur le poste nomade sitôt qu'elles ont été introduites dans le système d'information de l'organisme.
- Positionner un filtre de confidentialité sur les écrans des postes nomades dès qu'ils sont utilisés en dehors de l'organisme.
- Verrouiller l'appareil au bout de quelques minutes d'inactivité.

Notes

- De plus en plus d'ordinateurs portables sont équipés d'un dispositif de lecture d'empreinte digitale. La mise en œuvre de tels dispositifs est soumise à l'autorisation de la CNIL, sauf s'ils rentrent dans le cadre de l'Autorisation unique 52.
- Les utilisateurs ne doivent pas pouvoir désactiver le chiffrement de disque et de veiller à conserver une copie des clés quand le chiffrement est utilisé.

Outillage / Pour aller plus loin

- Voir le guide de l'ANSSI pour les voyages à l'étranger.

39.4 Spécificités pour les supports amovibles

Objectifs : réduire les risques liés au format et à l'utilisation des supports amovibles (clés USB, disques durs externes, CD, DVD, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Limiter l'usage des supports amovibles à ceux fournis par le service en charge de l'informatique.
- Interdire l'utilisation de clés USB à connexion sans fil (ex : Bluetooth).
- Interdire la connexion de clés USB sur des matériels non sécurisés (antivirus, pare-feu, etc.).
- Limiter l'utilisation des clés USB aux activités professionnelles.
- Désactiver la fonctionnalité d'exécution automatique sur tous les postes (stratégie de groupe).
- Chiffrer les données stockées sur un support amovible.
- Restituer les supports amovibles défectueux ou plus utiles au service en charge de l'informatique.
- Détruire de manière sécurisée les supports de données qui sont inutiles.
    - ♦ *Recommandations : utiliser un "dégausseur" pour les unités de stockage à technologie magnétique, un broyeur certifié au minimum classe 3 de la norme DIN 32757 pour les supports numériques tels que les CD et DVD, une technique appropriée pour les disques SSD / mémoires flash (ex : chiffrer le disque, le reformater, le re-chiffrer avec une clé différente), etc.*

Outillage / Pour aller plus loin

- Voir la note du CERTA sur les risques associés aux clés USB.

39.5 Spécificités pour les imprimantes et copieurs multifonctions

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Changer les mots de passe "constructeur" par défaut.
- Désactiver les interfaces réseau inutiles.
- Désactiver ou supprimer les services inutiles.
- Chiffrer les données sur le disque dur lorsque cette fonction est disponible.
- Limiter l'envoi de documents numérisés aux adresses de messagerie internes et dans certains cas limiter l'envoi de documents numérisés à une seule adresse de messagerie.
- Dans le cas d'une maintenance par un tiers, prévoir les mesures destinées à empêcher l'accès aux données.
    - ♦ *Recommandations : les données doivent être chiffrées ou effacées de manière sécurisée avant l'envoi en maintenance externe ; faire signer un engagement de confidentialité au mainteneur ou faire des réparations sur place en présence d'un membre du service en charge de l'informatique si les données sont sensibles et si elles ne peuvent pas être chiffrées ou effacées dans leur totalité (panne d'un disque dur, dysfonctionnement, etc.) ; interdire l'envoi en maintenance externe dans le cas de données sensibles, etc.*
- Dans le cas d'une télémaintenance par un tiers à une imprimante ou copieur multifonctions hébergé localement, prendre des mesures spécifiques pour protéger chaque accès.
    - ♦ *Recommandations : faire signer un engagement de confidentialité par le tiers externe, mettre en place de mots de passe robustes, spécifiques et renouvelés régulièrement, pour l'accès en télémaintenance, activer les accès entrant en télémaintenance uniquement sur demande, les accès entrant étant inactifs par défaut, journaliser les accès en télémaintenance, interdire les possibilités de rebond depuis l'accès en télémaintenance vers le reste du réseau local et plus largement vers internet, etc.*
- Empêcher l'accès à des données stockées sur des imprimantes ou copieurs multifonctions mis au rebut.
    - ♦ *Recommandations : entreposer l'équipement sur site dans un local sécurisé en attendant qu'il quitte l'organisme, utiliser un dispositif d'effacement sécurisé sur les données stockées sur les disques durs ou la mémoire intégrée ou détruire physiquement l'équipement si ce n'est pas possible (panne, dysfonctionnement, etc.), faire signer un accord de confidentialité dans le cas où la mise au rebut est réalisée par un tiers, émettre un procès-verbal de destruction des supports et le conserver pendant 10 ans.*

40 Sécurité des sites web

Objectifs : diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel (référentiel général de sécurité, chiffrement TLS des flux, politique de dépôt de cookies, audits de sécurité, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Si le site est un téléservice, celui-ci doit être conforme au référentiel général de sécurité (RGS). Pour cela, le site doit notamment utiliser un certificat signé par une autorité racine de confiance "qualifiée" (ex : LSTI, voir la liste des prestataires de certification électronique qualifiés) ;
  - ♦ *Recommandation : le certificat de conformité au RGS doit être présent sur le site.*
- Le chiffrement des flux doit être garanti par TLS, Dès lors, il est nécessaire de configurer le serveur web afin que celui-ci n'accepte que ce type de protocole (exclure notamment le protocole SSL et rendre le chiffrement obligatoire lors de la négociation SSL)
- Si vous utilisez des cookies :
  - ♦ Assurez vous d'avoir obtenu un consentement à leur dépôt, ♦ Pour les cookies, déposez depuis votre domaine :
    - ◊ Assurez vous de limiter la durée de validité des cookies à 13 mois,
    - ◊ Utilisez le flag HTTP-ONLY,
    - ◊ Utilisez le flag Same-Site pour les cookies qui n'ont pas besoin d'être accessible depuis une tierce partie.
- Définissez un Content-Secuirty-Policy n'incluant que les acteurs que vous autorisez à déposer des contenus sur votre site.
- Effectuez des audits de sécurité sur le site.

Outillage / Pour aller plus loin

- L'agence nationale de la sécurité des systèmes d'information (ANSSI) a mis à disposition un guide sur ce sujet, il est conseillé d'en suivre les recommandations.

41 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne

Objectifs : être conforme aux articles 68 et 69 de la loi informatique et libertés et les articles 44 à 50 du règlement général sur la protection des données (RGPD) ; respecter les obligations en matière de transfert de données en dehors de l'Union européenne.

Bonnes pratiques

- Détailler le lieu géographique de stockage des différentes données du traitement.
- En fonction du pays concerné, justifier le choix d'un hébergement éloigné et indiquer les modalités d'encadrement juridique mises en œuvre afin d'assurer une protection adéquate aux données faisant l'objet d'un transfert transfrontalier.

42 Traçabilité (journalisation)

Objectifs : assurer l'enregistrement et l'imputabilité des consultations et actions des utilisateurs du traitement, afin de pouvoir fournir des preuves dans le cadre d'enquêtes (système de journalisation, protection, analyse, conservation, etc.).

Bonnes pratiques dans le cas où la mesure est choisie pour traiter des risques

- Mettre en place un système de journalisation applicative permettant de conserver une trace des accès et modifications de données opérés par les utilisateurs et du moment où ils ont eu lieu.
    - ♦ *Recommandations : horodater les événements en prenant comme référence le temps UTC (Coordinated Universal Time), utiliser une source de temps fiable sur laquelle les systèmes se synchroniseront, telle qu'un serveur NTP (Network Time Protocol) ou une radiosynchronisation, centraliser localement (regrouper tous les journaux sur une machine de collecte relativement isolée et accompagnée d'un poste de travail de consultation dédié), exporter les journaux (envois planifiés, transfert automatique ou utilisation d'un réseau d'administration), disposer d'une capacité de stockage suffisante, se doter d'un système d'archivage et de sauvegarde pour les journaux d'événements, protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés, assurer la stricte confidentialité des journaux, etc.*
- Mettre en place une authentification des utilisateurs permettant d'assurer l'imputabilité des événements journalisés.
    - ♦ *Recommandations : interdire les identifiants génériques ou partagés, respecter les recommandations de la CNIL concernant les mots de passe, privilégier une authentification forte à deux facteurs, etc.*
- Respecter les exigences de la loi informatique et libertés concernant les événements journalisés rattachés à un utilisateur identifié.
    - ♦ *Recommandations : il est nécessaire d'informer les utilisateurs de la traçabilité mise en place, de l'inclure dans la déclaration du traitement à la CNIL et de ne pas utiliser les traces collectées pour d'autres finalités, etc.*
- Procéder périodiquement à l'analyse des informations journalisées, voire mettre en place un système de détection automatique de comportements anormaux.
- Conserver les journaux d'événements sur six mois, hors contraintes légales et réglementaires particulières imposant des durées de conservation spécifiques.

Outillage / Pour aller plus loin

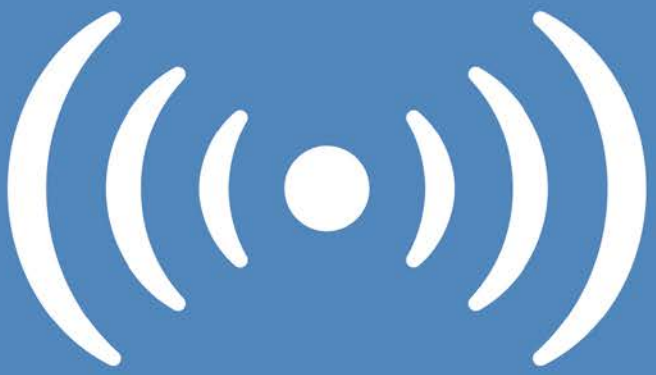
- En fonction de l'étude des risques et des contraintes légales, assurer la valeur probante des journaux par des mesures techniques (horodatage, signature

électronique, calcul d'empreinte?) conformes au référentiel général de sécurité (RGS).

Analyse d'impact relative à la protection des données

Privacy Impact Assessment (PIA)

APPLICATION AUX OBJETS CONNECTÉS



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Édition février 2018

Table des matières

Avant-propos

Ce document est une déclinaison des guides PIA de la CNIL au secteur spécifique des objets connectés.

Théoriquement mené par un responsable de traitement ou un fournisseur, un PIA a pour objectif de construire et de démontrer la mise en œuvre des principes de protection de la vie privée afin que les personnes concernées conservent la maîtrise de leurs données à caractère personnel.

Le fonctionnement itératif de cette méthode doit permettre de garantir une utilisation raisonnée et fiable de ces données dans le traitement.

Ce document est basé sur la méthode PIA de la CNIL

La méthode comporte trois guides, décrivant respectivement la démarche, les éléments pour formaliser l'étude et un guide de bonne pratiques pour la protection de la vie privée :

Ils sont téléchargeables sur le site de la CNIL et seront utiles pour remplir ce document :

https://www.cnil.fr/fr/PIA-privacy-impact-assessment

Ce document a la structure d'un rapport de PIA, qui est le livrable du PIA[1].

Certaines parties de ce document [zones grisées] sont renseignées à titre d'exemple, en se basant sur un produit générique fictif composé d'un jouet interactif servant également de *babyphone*, d'une application mobile et d'un service en ligne, dont les données personnelles sont stockées chez un hébergeur tiers et qui fait appel à des prestataires (interactivité, analyse des usages, régie publicitaire).

Également, des notes apportent des conseils ou soulignent des points de vigilance liés au contexte particulier des objets connectés.

Enfin, des encarts [zones beiges] apportent un accompagnement méthodologique au fil du document et permettent de renseigner les évaluations prévues.

[1] Voir les lignes directrices du G29 sur les PIA (en anglais).

1 Étude du contexte

Généralement réalisée par la maîtrise d'ouvrage[2], avec l'aide d'une personne en charge des aspects « Informatique et libertés »[3].

Objectif : obtenir une vision claire des traitements de données personnelles considérés.

1.1 Vue d'ensemble du traitement

- Présenter **le produit** considéré, sa **nature**, sa **portée**, son **contexte**, ses **finalités** et ses **enjeux**[4] de manière synthétique.
- Identifier le **responsable du traitement** et les éventuels **sous-traitants**.
- Recenser les **référentiels applicables** au traitement, utiles ou à respecter[5], notamment les codes de conduite approuvés (cf. art. 40 du [RGPD]) et certifications en matière de protection des données (cf. art. 42 du [RGPD])[6].

1.1.1 Description du produit

Le modèle de tableau ci-dessous peut être utilisé pour décrire le produit de manière synthétique.

Pour illustrer son utilisation, il est renseigné à partir d'un exemple de jouet fictif, qui servira tout au long du document.

Description du produit	L'appareil est un jouet disposant d'un micro, d'une caméra et de boutons pour des fonctions basiques (*power*, *action*, *reset*). Il se connecte en Wifi et communique avec une application mobile dédiée, hébergée sur un *smartphone* ou une tablette, et avec un service en ligne.
Finalités du traitement	Fournir une interactivité à l'enfant, à travers la possibilité de dialogue avec le jouet (questions/réponses en langage naturel par reconnaissance vocale). Permettre à l'enfant de communiquer en ligne (envoi de messages vocaux, de textes et de photos) avec ses amis et/ou ses parents. Remonter des informations aux parents (dispositif de surveillance).
Enjeux du traitement	Créer une nouvelle classe de jouets destinés aux enfants et à leurs parents, en tirant partie de la connectivité, tout en respectant le cadre légal et la sécurité des données personnelles.
Responsable du traitement	Société *Fab* (fabricant)
Sous-traitant(s)	Société *Héb* (hébergeur), Société *Int* (moteur d'interactivité), Société *AnaPub* (analyse d'usages et régie publicitaire)

[2] Il s'agit des métiers. Elle peut être déléguée, représentée ou sous-traitée.
[3] Correspondant Informatique et libertés, délégué à la protection des données, ou autre.
[4] Répondre à la question « Quels sont les bénéfices attendus (pour l'organisme, pour les personnes concernées, pour la société en général, *etc.*) ? ».
[5] Selon les cas, ils serviront notamment à démontrer le respect de principes fondamentaux, à justifier des mesures ou à prouver qu'elles correspondent à l'état de l'art.
[6] Autres exemples : politique de sécurité, normes juridiques sectorielles, etc.

1.1.2 Référentiels sectoriels applicables au traitement[7]

Vous trouverez ci-dessous un tableau permettant de détailler les référentiels sectoriels applicables à votre traitement[8] ainsi que les modalités de leur prise en compte.

Référentiels applicables au traitement	Prise en compte

1.2 Données, processus et supports

- Délimiter et décrire le périmètre de manière détaillée :
  - les **données** personnelles concernées, leurs **destinataires**[9] et **durées de conservation** ;
  - une description des **processus** et des **supports** de données pour l'ensemble du cycle de vie des données (depuis leur collecte jusqu'à leur effacement).

1.2.1 Données traitées

Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les données traitées et les personnes qui y accèdent.

Pour illustrer son utilisation, il est renseigné avec les données de notre exemple de jouet fictif.

Données à caractère personnel	Catégories	Destinataires	Personnes pouvant y accéder
Informations sur l'utilisateur : prénom, date de naissance, genre, adresse électronique, numéro de téléphone	Données courantes : données d'identification	Société *Héb*	Personnels habilités des Sociétés *Fab* et *Héb*
Données renseignées dans une application tierce (Twitter, Facebook, *etc.*), obtenues par lien avec le compte utilisateur	Données courantes : données d'identification	Société *Héb*	Personnels habilités des Sociétés *Fab* et *Héb*
Données relevées : textes/messages, sons, images, mouvements, température, humidité Journaux d'usage de l'appareil, de l'application mobile et du service en ligne	Données courantes : habitudes de vie Données perçues comme sensibles : image et voix (permettant des traitements biométriques) Données sensibles (au sens du GDPR) : données liées à des mineurs	Société Héb + Sociétés *Int* et *AnaPub*	Personnels habilités des Sociétés *Fab* et *Héb* + Personnels habilités des Sociétés *Int* et *AnaPub*

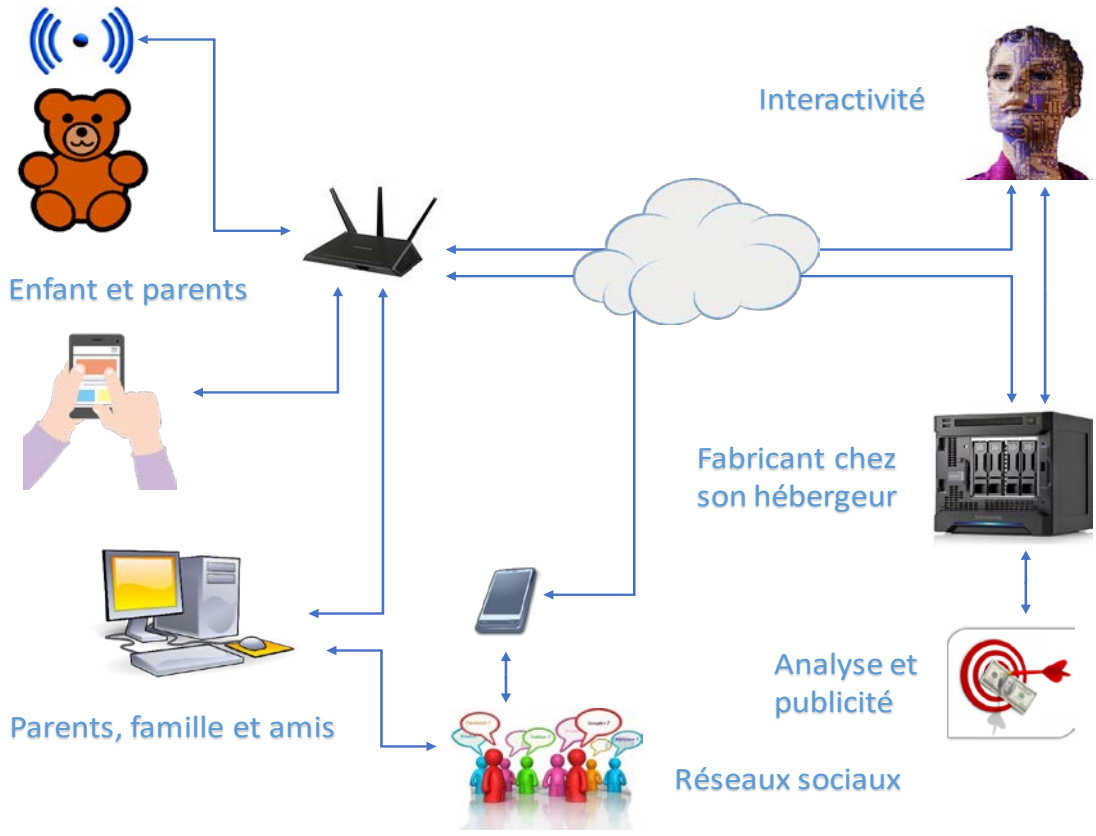
[7] Voir article 35 (8) du [RGPD].
[8] Par ex., un code de conduite, une certification, une politique générale de sécurité, un *PIA Framework*, etc.
[9] Définition de « destinataire » - voir article 4(9) du RGPD.

Données à caractère personnel	Catégories	Destinataires	Personnes pouvant y accéder
Données calculées : réponses aux questions des enfants et identification des centres d'intérêts pour aider à la pertinence des réponses Analyse des usages et publicités ciblées	Données courantes : habitudes de vie Données sensibles (au sens du RGPD) : données liées à des mineurs	Sociétés *Int* et *AnaPub* + Société *Héb*	Personnels habilités des Sociétés *Int* et *AnaPub* + Personnels habilités des Sociétés *Fab* et *Héb*

1.2.2 Cycle de vie des données et processus

Vous devez ici représenter et décrire le fonctionnement général du produit, avec un schéma des flux de données et la description détaillée des processus mis en œuvre.

À titre d'exemple, vous trouverez ci-dessous le schéma de fonctionnement de notre jouet fictif.



Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les processus de traitement de données mis en œuvre.

Pour illustrer son utilisation, il est renseigné avec notre exemple de jouet fictif.

Processus	Description détaillée du processus
1. Enregistrer un compte	L'utilisateur fournit des données d'identification à l'ouverture de son compte
2. Capter les données	Des données sont relevées via des capteurs
3. Transférer vers le mobile	Les données sont transférées vers l'application mobile, directement par l'appareil ou à travers les serveurs *cloud*
4. Saisir des données	Des données sont saisies dans l'application mobile
5. Stocker dans le mobile	Les données sont stockées dans l'application mobile
6. Envoyer les données aux serveurs	Les données sont envoyées aux serveurs *cloud*, par l'appareil directement ou par l'application mobile
7. Générer l'interactivité	Le moteur d'interactivité dans le *cloud* génère les données de réponse, en se basant sur les dialogues précédents et la détection des centres d'intérêt
8. Envoyer des données au jouet	Les données d'interactivité sont renvoyées à l'appareil, directement ou à travers l'application mobile
9. Conserver les données sur les serveurs	Les données captées et calculées sont stockées sur les serveurs *cloud*
10. Analyser les données	Des algorithmes d'analyse des données sont exécutés sur les serveurs *cloud* pour produire des statistiques d'usage ainsi qu'un ciblage publicitaire
11. Consulter les données des serveurs *cloud*	Une partie des données captées et calculées peuvent être consultées via l'application mobile ou sur un espace Internet personnel
12. Partager des données	Certaines données peuvent être relayées vers des applications tierces ou postées sur des réseaux sociaux

1.2.3 Supports des données

Vous trouverez ci-dessous un tableau permettant de lister de manière détaillée les supports des données. Pour illustrer son utilisation, il est renseigné avec notre exemple de jouet fictif.

Systèmes informatiques[10] sur lesquels reposent les données	Autres supports[11]
- Appareil (caméra, micro, haut-parleur, capteurs de mouvement, température, humidité) - *Smartphone/tablette/ordinateur* de l'utilisateur - Application mobile/navigateur - Réseau Wifi - Internet - Serveurs *cloud* de *Héb*, *Int et AnaPub*	- Utilisateur - Locaux de l'utilisateur - Locaux de *Fab* et *Héb* - Personnels de *Fab* et *Héb* - Locaux de *Int* et *AnaPub* - Personnels de *Int* et *AnaPub*

Attention : toute la partie 1 « Contexte » devra être relue par le CIL ou le DPD afin de s'assurer qu'elle est exhaustive et reflète bien la réalité du terrain.

Cette relecture est d'autant plus nécessaire que cette partie décrit des éléments structurants pour les chapitres suivants.

[10] Décomposables en matériels (et supports de données électroniques), logiciels et canaux informatiques.
[11] Décomposables en personnes, supports papier et canaux de transmission papier.

2 Étude des principes fondamentaux

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge des aspects « Informatique et libertés ».

Objectif : bâtir le dispositif de conformité aux principes de protection de la vie privée.

Les principes fondamentaux de la protection de la vie privée qui doivent être pris en compte sont les suivants : finalité(s) de collecte des données déterminées et explicites, licéité du traitement, minimisation des données, qualité des données, durées de conservation limitées, information des personnes, recueil de leur consentement, possibilité d'accès direct à leurs données, portabilité de leurs données, possibilité de rectification et de suppression de leurs données sur demande, possibilité de s'opposer au traitement ou de le limiter, encadrement de la sous-traitance et des transfert de données en dehors de l'Union européenne.

- Expliciter et justifier les **choix effectués** et décrire les **mesures retenues** (existantes ou prévues) **pour respecter ces exigences légales** (nécessitant d'expliquer comment il est prévu de les mettre en œuvre).
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer la manière dont chaque point est prévu, explicité et justifié, conformément au [RGPD].
- Le cas échéant, revoir leur description ou proposer des mesures complémentaires.

Note : Vous trouverez au §2.3 un tableau pour récapituler la justification de l'ensemble de ces points et y consigner leur évaluation et les éventuelles mesures correctives.

2.1 Mesures garantissant la proportionnalité et la nécessité du traitement

2.1.1 Finalités : déterminées, explicites et légitimes[12]

Vous trouverez ci-dessous un tableau permettant de détailler les finalités de traitement des données et justifier leur légitimité[13].

Finalités	Légitimité

Note : penser à expliciter les finalités de partage avec des tiers, notamment pour la publicité et les « offres partenaires », ainsi que les finalités de traitement de données pour l'amélioration du service.

Note : penser à expliciter les modalités particulières du traitement, en précisant notamment les croisements de données s'il y a lieu.

[12] Voir article 5.1 (b) du [RGPD].

[13] Sur la légitimité de la finalité, voir l'avis WP 203 du G29 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Attention[14] : en raison de la vulnérabilité générale d'un enfant et compte tenu du fait que les données à caractère personnel doivent être traitées de manière loyale et licite, les responsables d'un traitement ciblant les enfants devraient respecter de façon encore plus stricte les principes de limitation de la finalité.

Plus particulièrement, les responsables du traitement ne devraient pas utiliser les données de l'enfant à des fins de profilage (par ex. pour de la publicité ciblée), que ce soit directement ou indirectement, dans la mesure où une telle pratique n'entre pas dans la sphère de compréhension d'un enfant et dépasse dès lors les limites d'un traitement loyal.

2.1.2 Fondement : licéité du traitement, interdiction du détournement de finalité[15]

Vous trouverez ci-dessous la liste des critères de licéité. Un traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

Critères de licéité	Applicable	Justification
La personne concernée a consenti[16] au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques		
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci		
Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis		
Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique		
Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement		
Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[17]		

Note : dans le cas d'une obligation légale ou d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, préciser dans la justification le fondement légal du traitement dans le droit de l'Union européenne ou de l'État membre auquel le responsable du traitement est soumis.

Note : il peut y avoir plusieurs fondements pour un traitement : par exemple, un contrat lié à l'achat du produit pour son utilisation dans sa finalité principale et un consentement pour ses finalités secondaires (amélioration du service, marketing, *etc.*) qui sera recueilli lors de l'activation du produit.

[14] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[15] Voir article 6 du [RGPD].
[16] Concernant le recueil du consentement de la personne et son information, voir le chapitre 2.2.
[17] Ce point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions

Attention : si les données sont traitées à une fin autre que celle pour laquelle elles ont été collectées et que le traitement n'est pas fondé sur le consentement de la personne concernée ou sur le droit de l'Union européenne ou d'un État membre, il est nécessaire de déterminer si cette autre fin est compatible avec la finalité initiale de collecte, en tenant compte, entre autres :

- de l'existence éventuelle d'un lien entre la finalité du traitement et la finalité initiale de collecte des données ;
- du contexte de collecte initiale, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données ou des données relatives à des condamnations pénales et à des infractions[18] ;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

2.1.3 Minimisation des données : adéquates, pertinentes et limitées[19]

Il est important de réduire la gravité des risques en minimisant le nombre de données à caractère personnel qui seront traitées, en se limitant au strict nécessaire au regard de la finalité définie (ne pas les collecter sinon). Ensuite, il est également possible de minimiser les données elles-mêmes, par des mesures destinées à réduire leur sensibilité (cf. annexe 1 - Liste de mesures de minimisation des données).

Vous trouverez ci-dessous un tableau permettant de lister les données traitées, réduites au strict nécessaire, accompagnées de la justification du besoin et des éventuelles mesures de minimisation complémentaires.

Pour illustrer son utilisation, il est renseigné avec les données tirées de notre exemple de jouet fictif.

Types de données	Catégories de données	Détail des données traitées	Justification du besoin et de la pertinence des données	Mesures de minimisation
Données courantes	État-civil, identité, données d'identification	Prénom, date de naissance, genre, adresse électronique, numéro de téléphone, lien avec un compte de réseau social	Éléments nécessaires à la création d'un profil permettant de communiquer	Pas de nom de famille Remplacement de la date de naissance par l'âge ou une tranche d'âge Stockage séparé des données identifiantes, dans une base chiffrée
	Vie personnelle (habitudes de vie, situation familiale, hors données sensibles ou dangereuses, *etc.*)	Textes/messages, sons, images, mouvements, température, humidité Réponses aux questions des enfants, identification des centres d'intérêts pour aider à la pertinence des réponses, publicités ciblées	Éléments faisant partie des fonctions de communication	

[18] Voir articles 9 et 10 du [RGPD].
[19] Voir article 5.1 (c) du [RGPD].

Types de données	Catégories de données	Détail des données traitées	Justification du besoin et de la pertinence des données	Mesures de minimisation
	Vie professionnelle (CV, scolarité formation professionnelle, distinctions, *etc.*)	Non collectées		
	Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, *etc.*)	Non collectées		
	Données de connexion (adresses IP, journaux d'événements, *etc.*)	Traces applicatives Logs techniques	Besoins de sécurité et de vérifier le respect des CGU	Pseudonymisation pour l'exploitation statistique
	Données de localisation (déplacements, données GPS, GSM, *etc.*)	Localisation du *smartphone* intégrée dans les photos (si l'option est activée)	Inutile	Retrait des informations de localisation avant envoi des photos
Données perçues comme sensibles	Numéro de sécurité sociale (NIR)	Non collecté		
	Données biométriques	Données brutes : voix et photographies	Éléments faisant partie des fonctions de communication	
	Données bancaires	Non collectées		
Données sensibles [20]	Opinions philosophiques, politiques, religieuses, syndicales, vie sexuelle, données de santé, origine raciales ou ethniques, relatives à la santé ou à la vie sexuelle	Non collecté mais peuvent apparaître directement ou indirectement dans les données textes, audios et vidéos	Éléments faisant partie des fonctions de communication	
	Infractions, condamnations, mesures de sécurité	Non collecté		

Notes : penser à bien justifier la collecte de certaines données (localisation, date de naissance, âge, poids, *etc.*) et à bien faire la distinction entre les données anonymes et pseudonymes.

[20] Voir notamment les articles 9 et 10 du [RGPD]. Des restrictions d'usage et des formalités particulières sont à prendre en compte.

Conseil : éviter les champs de saisie en texte libre (ex : zones « commentaires »), en raison du risque que les utilisateurs y consignent des informations ne respectant pas les principes de minimisation. On préférera donc des champs de saisie à base de listes déroulantes. Si on ne peut éviter la saisie de texte libre, une sensibilisation des utilisateurs devra être faite quant à l'usage de ces champs, vis-à-vis des conditions générales du service et vis-à-vis de la loi (pas de propos injurieux, pas de données sensibles non déclarées, *etc.*).

Attention : pour un traitement concernant des personnes mineures, les données sont globalement considérées comme sensibles selon le [RGPD].

Attention[21] : en raison de la vulnérabilité générale d'un enfant et compte tenu du fait que les données à caractère personnel doivent être traitées de manière loyale et licite, les responsables d'un traitement ciblant les enfants devraient respecter de façon encore plus stricte les principes de minimisation des données et de limitation de la finalité.

Les responsables du traitement devraient s'abstenir plus spécifiquement de collecter des données relatives aux parents ou aux membres de la famille de l'enfant, telles que des informations financières ou des catégories particulières d'information comme des données médicales.

2.1.4 Qualité des données : exactes et tenues à jour[22]

Vous trouverez ci-dessous un tableau permettant de détailler les mesures de respect de la qualité des données, mises en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour la qualité des données	Appareil	Application mobile	Espace personnel	Justification
Vérification régulière de l'exactitude des données personnelles de l'utilisateur				
Invitation de l'utilisateur à contrôler et, si nécessaire, mettre à jour ses données				
Traçabilité des modifications des données				

2.1.5 Durées de conservation : limitées[23]

Une durée de conservation doit être définie pour chaque type de données et justifiée par les besoins du traitement et/ou des contraintes légales. On distingue ainsi les données courantes et les données archivées dont l'accès sera restreint aux seuls acteurs concernées.

Un mécanisme de suppression doit être implémenté pour archiver les données courantes ou purger les données archivées à la fin de leur période de conservation. Les traces fonctionnelles devront également être purgées, tout comme les logs techniques qui ne pourront pas être conservés indéfiniment.

Notes : En réduisant la quantité de données traitées et disponibles, l'archivage et la purge permettent de limiter les impacts en cas de vol ou de diffusion accidentelle de la base de données.

Afin de s'assurer de l'effectivité de ces durées de conservation, il est conseillé de mettre en place un mécanisme automatique basé sur la date de création des données ou de leur dernier usage.

[21] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[22] *Voir article 5.1 (d) du* [RGPD]. *L'exigence de qualité porte également sur le lien entre les données qui identifient les personnes et les données qui les concernent.*
[23] Voir article 5.1 (e) du [RGPD], à défaut d'une autre obligation légale imposant une conservation plus longue.

Attention : Pour les données sensibles, pour les données à risques élevé, il conviendra d'utiliser des outils d'effacement sécurisés rendant les données irrécupérables.

Les durées de conservation, leur justification et les mécanismes de purge peuvent être présentés dans le tableau ci-dessous.

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données courantes			
Données archivées			
Traces fonctionnelles			
Journaux techniques (*logs*)			

2.2 Mesures protectrices des droits des personnes des personnes concernées

2.2.1 Information des personnes concernées (traitement loyal et transparent)[24]

Si le traitement bénéficie d'une exemption au droit d'information, prévue par les articles 12, 13 et 14 du [RGPD], vous le justifierez ci-dessous.

Dispense d'information des personnes concernées	Justification

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer l'information des utilisateurs (ou de leurs parents)[25].

Vous y détaillerez leur mise en œuvre (de préférence en joignant des copies d'écrans et extraits de documents) sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou sur l'impossibilité de leur mise en œuvre.

Mesures pour le droit à l'information	Appareil	Application mobile	Espace personnel	Justification
Présentation, lors de l'initialisation du dispositif, des conditions d'utilisation/confidentialité				
Possibilité d'accéder aux conditions d'utilisation/confidentialité après l'initialisation				
Conditions lisibles et compréhensibles				
Existence de clauses spécifiques au dispositif				
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, *etc.*)				

[24] Voir articles 12, 13 et 14 du [RGPD].
[25] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».

Mesures pour le droit à l'information	Appareil	Application mobile	Espace personnel	Justification
Présentation détaillée des données personnelles collectées				
Présentation des éventuels accès à des identifiants de l'appareil, du *smartphone*/tablette ou de l'ordinateur, en précisant si ces identifiants sont communiqués à des tiers				
Présentation des droits de l'utilisateur (retrait du consentement, suppression de données, *etc.*)				
Information de l'utilisateur si l'application est susceptible de fonctionner en arrière-plan				
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation				
Information sur les protections d'accès à l'appareil				
Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité				
Information sur la possibilité de définir des directives relatives au sort des données post-mortem				
Le cas échéant, information de l'utilisateur de tout changement concernant les données collectées, les finalités, les clauses de confidentialité				
Dans le cas de transmission de données à des tiers :				
- présentation détaillée des finalités de transmission à des tiers				
- présentation détaillée des données personnelles transmises				
- indication de l'identité des organismes tiers				

Attention : dans le cas de transmission de données à des organismes tiers au responsable du traitement (filiales, affiliés, intragroupe, partenaires, *etc.*), il est nécessaire de fournir la liste des destinataires (dans une rubrique d'information dédiée), en précisant les catégories de données transmises et la finalité du transfert, et en fournissant un lien hypertexte vers la politique de protection des données des destinataires respectifs. Il faut également prévoir un processus interne permettant de mettre à jour cette liste en cas de modification.

Attention[26] : les développeurs d'applications, en collaboration avec les magasins d'applications et les fabricants de systèmes d'exploitation et de dispositifs, devraient présenter les informations utiles de manière simple, dans un langage adapté à un jeune âge, éventuellement par un message sonore.

[26] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.

Recommandation : placer un « *QR Code* » d'information sur l'objet et responsabiliser les utilisateurs (ou leurs parents) pour qu'ils informent les tiers que leurs données sont susceptibles d'être collectées (par ex. les autres enfants conversant avec l'appareil ou présents sur les photos partagées).

2.2.2 Recueil du consentement, le cas échéant : exprès

Si le traitement est fondé sur le consentement de la personne, le responsable de traitement doit être en mesure de démontrer qu'il a bien recueilli ce consentement. La personne concernée doit avoir la possibilité de retirer son accord à tout moment et de façon simple[27].

Si la licéité du traitement[28] repose sur le consentement, vous trouverez ci-dessous une liste de mesures destinées à assurer le recueil du consentement des utilisateurs (ou de leurs parents)[29], le rappel et la réaffirmation de leur consentement, ainsi que le maintien des paramètres liés à celui-ci.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour le recueil du consentement	Appareil	Application mobile	Espace personnel	Justification
Consentement exprès lors de l'initialisation				
Consentement segmenté par catégorie de données ou types de traitement				
Consentement exprès avant le partage de données avec d'autres utilisateurs				
Consentement présenté de manière simple, compréhensible et adaptée à l'utilisateur cible (notamment pour les enfants)				
Recueil du consentement des parents pour les mineurs de moins de 13 ans				
Pour un nouvel utilisateur, mise en œuvre d'un nouveau recueil de consentement				
Après une longue période sans utilisation, demande à l'utilisateur de réaffirmer son consentement				
Si l'utilisateur a consenti au traitement de données particulières (par ex. sa localisation), l'interface signale clairement que ce traitement a lieu (icône, voyant lumineux)				
Si l'utilisateur change d'appareil, de *smartphone* ou d'ordinateur, s'il réinstalle l'application mobile ou efface ses *cookies*, les paramètres liés à son consentement sont maintenus				

Attention[30] : le RGPD a renforcé les bases légales concernant le consentement pour toute offre directe de services de la société de l'information à destination des mineurs, et la charge de la preuve (non ambigüe) incombe au responsable de traitement ou au sous-traitant.

[27] Voir articles 7 et 8 du [RGPD].
[28] Concernant la licéité du traitement, voir le chapitre 2.1.
[29] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».
[30] Voir article 8 du [RGPD].

En pratique, le consentement du responsable parental est requis pour les enfants de moins de 16 ans, avec la possibilité pour les États membres de fixer un âge inférieur, mais qui ne peut être en deçà de 13 ans. Le responsable du traitement s'efforce raisonnablement de vérifier que le consentement est bien donné par le responsable parental, compte tenu des moyens technologiques disponibles.

Attention[31] : Lorsque le consentement d'un mineur peut être légalement obtenu et que l'application est destinée à l'utilisation par un enfant ou un mineur, le responsable du traitement doit être attentif au fait que le mineur peut avoir une compréhension limitée du traitement des données et qu'il n'accorde que peu d'attention aux informations sur le sujet.

Les développeurs d'applications, en collaboration avec les magasins d'applications et les fabricants de systèmes d'exploitation et de dispositifs, devraient présenter les informations utiles de manière simple, dans un langage adapté à un jeune âge.

2.2.3 Exercice des droits d'accès[32] et à la portabilité[33]

Si le traitement bénéficie d'une exemption au droit d'accès, prévue par l'article 15 du [RGPD], vous le justifierez ci-dessous.

Exemption du droit d'accès	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit d'accès des utilisateurs (ou de leurs parents) à l'ensemble des données à caractère personnel les concernant.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour le droit d'accès	Appareil	Application mobile	Espace personnel	Justification
Possibilité d'accéder à l'ensemble des données personnelles de l'utilisateur, via les interfaces courantes				
Possibilité de consulter, de manière sécurisée, les traces d'utilisation liées à l'utilisateur				
Possibilité de télécharger une archive de l'ensemble des données à caractère personnel liées à l'utilisateur				

Enfin, si le droit à la portabilité s'applique au traitement conformément à l'article 20 du [RGPD], vous en détaillerez la mise en œuvre ci-dessous.

[31] Voir l'avis 02/2013 du G29 sur les applications destinées aux dispositifs intelligents.
[32] Voir article 15 du [RGPD].
[33] Voir article 48 de la Loi 2016-1321 du 7 octobre 2016 pour une République numérique et article 20 du [RGPD].

Mesures pour le droit à la portabilité	Appareil	Application mobile	Espace personnel	Justification
Possibilité de récupérer, sous une forme aisément réutilisable, les données personnelles qui ont été fournies par l'utilisateur, afin de pouvoir les transférer à un service tiers				

2.2.4 Exercice des droits de rectification et d'effacement[34]

Si le traitement bénéficie d'une exemption au droit de rectification et d'effacement, prévue par l'article 17 du [RGPD] vous le justifierez ci-dessous.

Exemption des droits de rectification et d'effacement	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit à la rectification ou l'effacement des données des utilisateurs (ou de leurs parents[35]) qui le souhaitent.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour les droits de rectification et d'effacement	Appareil	Application mobile	Espace personnel	Justification
Possibilité de rectifier les données personnelles				
Possibilité de supprimer les données personnelles				
Indication des données personnelles qui seront conservées malgré tout (contraintes techniques, obligations légales, *etc.*)				
Mise en œuvre du droit à l'oubli pour les mineurs				
Indications claires et étapes simples pour effacer les données avant de mettre l'appareil au rebut				
Conseils fournis pour remise à zéro en cas de vente de l'appareil				
Possibilité d'effacer les données en cas de vol de l'appareil				

Attention[36] : Le responsable de traitement dispose d'un délai d'un mois pour effacer les données ou répondre à la personne ; passé ce délai, la personne concernée peut saisir la CNIL. Des exceptions

[34] Voir articles 16, 17 et 19 du [RGPD].
[35] Voir sur le site de la CNIL : « Editeurs de sites pour enfants : n'oubliez pas vos obligations ! ».
[36] Voir la Loi 2016-1321 du 7 octobre 2016 pour une République numérique modifiant l'article 40 de la [Loi-I&L], qui complète le « droit à l'oubli » prévu par l'article 17 du [RGPD].

existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement et sans autre motif demander au site l'effacement, dans les meilleurs délais, des données le concernant.

2.2.5 Exercice des droits de limitation du traitement et d'opposition[37]

Si le traitement bénéficie d'une exemption au droit de limitation et d'opposition, prévue par l'article 21 du [RGPD], vous le justifierez ci-dessous.

Exemption des droits de limitation et d'opposition	Justification	Modalités de réponse aux personnes concernées

Dans le cas contraire, vous trouverez ci-dessous une liste de mesures destinées à assurer le droit d'opposition et de limitation soit sur les différentes finalités soit sur l'ensemble d'un traitement.

Vous y détaillerez leur mise en œuvre sur l'appareil, l'application mobile et l'espace personnel, ainsi qu'une justification sur les modalités ou l'impossibilité de mise en œuvre.

Mesures pour les droits de limitation et d'opposition	Appareil	Application mobile	Espace personnel	Justification
Existence de paramètres « Vie privée »				
Invitation à changer les paramètres par défaut				
Paramètres « Vie privée » accessibles pendant l'initialisation du dispositif				
Paramètres « Vie privée » accessibles après l'initialisation du dispositif				
Existence d'un dispositif de contrôle parental pour les enfants de moins de 13 ans				
Existence d'un dispositif permettant à l'utilisateur de demander la limitation du traitement				
Existence de moyens techniques permettant au RT de verrouiller l'accès et l'utilisation des données objet de la limitation				
Possibilité de désactiver certaines fonctions de l'appareil (micro, navigateur web, *etc.*)				
Existence d'applications alternatives pour accéder à l'appareil				
Possibilité de s'opposer au fonctionnement de l'application mobile en arrière-plan				

[37] Voir articles 18 et 21 du [RGPD].

Mesures pour les droits de limitation et d'opposition	Appareil	Application mobile	Espace personnel	Justification
Conformité en matière de traçage (*cookies*, publicité, *etc.*)				
Exclusion des enfants de moins de 13 ans des traitements de profilage automatisé				
Exclusion effective de traitement des données de l'utilisateur en cas de retrait du consentement				

Note : le droit à la limitation permet à la personne concernée d'exiger le « gel » du traitement de ses données, comme mesure conservatoire le temps d'en vérifier la légitimité, par exemple.

2.2.6 Sous-traitance : identifiée et contractualisée[38]

Un contrat de sous-traitance doit être conclu avec chacun des sous-traitants, précisant l'ensemble des éléments prévus à l'art. 28 du [RGPD] : durée, périmètre, finalité, des instructions de traitement documentées, l'autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve du respect du [RGPD], notification dans les meilleurs délais de toute violation de données, *etc.*

Vous trouverez ci-dessous un tableau permettant de détailler les contrats pour chacun des sous-traitants.

Nom du sous-traitant	Finalité	Périmètre	Référence du contrat	Conformité art.28

2.2.7 Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne[39]

Vous trouverez ci-dessous un tableau permettant de détailler le lieu géographique de stockage des données de l'appareil, de l'application mobile et de l'espace personnel dans le *cloud*.

En fonction du pays concerné, vous devrez justifier le choix d'un hébergement éloigné et indiquer les modalités d'encadrement juridique mises en œuvre afin d'assurer une protection adéquate aux données faisant l'objet d'un transfert transfrontalier.

Lieu de stockage des données	France	Union européenne	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)
Données de l'appareil					

[38] Voir article 28 du [RGPD].
[39] Voir articles 44 à 50 du [RGPD].

Lieu de stockage des données	France	Union européenne	Pays reconnu adéquat par l'UE	Autre pays	Justification et encadrement (clauses contractuelles types, règles internes d'entreprise)
Données de l'application mobile					
Données de l'espace personnel					

2.3 Évaluation du respect des principes fondamentaux

Vous trouverez ci-dessous un tableau permettant, pour chacun des points de respect des exigences légales, de résumer la manière dont il est appliqué dans le traitement.

Les deux dernières colonnes sont destinées à l'évaluateur :

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures permettent de respecter les principes fondamentaux.

→ Mesures correctives :

Le cas échéant, il indiquera les mesures complémentaires qui seraient nécessaires.

Mesures garantissant la proportionnalité et la nécessité du traitement	Justification	Acceptable / améliorable ?	Mesures correctives
Finalités : déterminées, explicites et légitimes			
Fondement : licéité du traitement, interdiction du détournement de finalité			
Minimisation des données : adéquates, pertinentes et limitées			
Qualité des données : exactes et tenues à jour			
Durées de conservation : limitées			
Mesures protectrices des droits des personnes concernées	**Justification**	**Acceptable / améliorable ?**	**Mesures correctives**
Information des personnes concernées (traitement loyal et transparent)			
Recueil du consentement			
Exercice du droit d'accès et droit à la portabilité			
Exercice des droits de rectification et d'effacement			
Exercice des droits de limitation du traitement et d'opposition			
Sous-traitance : identifiée et contractualisée			
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne			

3 Étude des risques liés à la sécurité des données[40]

Un risque est un scénario hypothétique qui décrit un événement redouté et toutes les menaces qui permettraient qu'il survienne. Plus précisément, il décrit :

- comment des sources de risques (ex. : un salarié soudoyé par un concurrent)
- pourraient exploiter les vulnérabilités des supports de données (ex. : le système de gestion des fichiers, qui permet de manipuler les données)
- dans le cadre de menaces (ex. : détournement par envoi de courriers électroniques)
- et permettre à des événements redoutés de survenir (ex. : accès illégitime à des données)
- sur les données à caractère personnel (ex. : fichier des clients)
- et ainsi provoquer des impacts sur la vie privée des personnes concernées (ex. : sollicitations non désirées, sentiment d'atteinte à la vie privée, ennuis personnels ou professionnels).

3.1 Évaluation des mesures existantes ou prévues

Généralement réalisé par la maîtrise d'œuvre[41], puis évaluée par une personne en charge de la sécurité de l'information[42] notamment le responsable de la sécurité des systèmes d'information si désigné.

Objectif : obtenir une bonne connaissance des mesures contribuant à la sécurité.

- Identifier ou déterminer les **mesures existantes ou prévues** (déjà engagées), qui peuvent être de trois natures différentes :
  1. **mesures portant spécifiquement sur les données du traitement** : chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, *etc.* ;
  2. **mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** : sécurité de l'exploitation, sauvegardes, sécurité des matériels, *etc.* ;
  3. **mesures organisationnelles (gouvernance)** : politique, gestion des projets, gestion des personnels, gestion des incidents et violations, relations avec les tiers, *etc.*
- Vérifier qu'il n'est pas utile, ou pas possible, d'améliorer chaque mesure et sa description, conformément aux bonnes pratiques de sécurité.
- Le cas échéant, préciser leur description ou proposer des mesures complémentaires.

Notes : Les catégories de mesures de sécurité ci-dessous correspondent aux bonnes pratiques recommandées par la CNIL[43].

Vous devrez également tenir compte des référentiels sectoriels applicables à votre traitement[44] (politique générale de sécurité, *PIA Framework*, code de conduite, *etc.*).

Note : Vous trouverez au §3.1.4 un tableau pour récapituler la mise en œuvre de l'ensemble de ces mesures et y consigner leur évaluation et les éventuelles mesures correctives.

[40] Voir article 32 du [RGPD].
[41] Elle peut être déléguée, représentée ou sous-traitée.
[42] Responsable de la sécurité des systèmes d'information ou autre.
[43] Voir le Guide sécurité des données personnelles de la CNIL.
[44] Voir article 35 (8) du [RGPD].

3.1.1 Mesures portant spécifiquement sur les données du traitement

Chiffrement

*Décrivez ici les **moyens mis en œuvre pour assurer la confidentialité des données** conservées (en base de données, dans des fichiers plats, les sauvegardes, etc.), ainsi que les modalités de gestion des clés de chiffrement (création, conservation, modification en cas de suspections de compromission, etc.).*

Détaillez les moyens de chiffrement employés pour les flux de données (VPN, TLS, etc.) mis en œuvre dans le traitement.

Notes : penser à la sécurité du Wifi (chiffrement, stockage du mot de passe Wifi).

Penser à la sécurisation des certificats, stockés sur l'appareil ou le *smartphone*, utilisés pour authentifier et chiffrer les connexions.

Anonymisation

Indiquez ici si des mécanismes d'anonymisation sont mis en œuvre, lesquels et à quelle fin.

Note : penser à bien faire la distinction entre les données anonymes et pseudonymes.

Cloisonnement des données (par rapport au reste du système d'information)

Indiquez ici si un cloisonnement du traitement est prévu, et comment il est réalisé.

Contrôle des accès logiques

*Indiquez ici comment les **profils utilisateurs** sont définis et attribués.*

*Précisez les moyens d'**authentification** mis en œuvre[45].*

*Le cas échéant, précisez les règles applicables aux **mots de passe** (longueur minimale, structure obligatoire, durée de validité, nombre de tentatives infructueuses avant blocage du compte, etc.).*

Notes : penser à la sécurité du mot de passe utilisateur, que ce soit sur l'appareil, sur le *smartphone* ou dans le *cloud*. Les mots de passe doivent être stockés sous forme hachée par un algorithme robuste avec application préalable d'un sel.

Penser à la protection de l'accès à l'application sur *smartphone* par mot de passe spécifique.

Penser à sécuriser l'appairage entre l'appareil, l'application mobile et l'espace personnel.

Penser à protéger les données, y compris les métadonnées (dont Exif) et traces techniques, en cas d'accès direct par connexion physique à l'appareil ou au *smartphone*.

[45] Voir la délibération de la CNIL n°2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe.

Traçabilité (journalisation)

*Indiquez ici si des **événements sont journalisés** et la durée de conservation de ces traces.*

Contrôle d'intégrité

Le cas échéant, indiquez ici si des mécanismes de contrôle d'intégrité des données stockées sont mis en œuvre, lesquels et à quelle fin. *Détaillez les mécanismes de contrôle d'intégrité employés sur les flux de données.*

Archivage

Le cas échéant, décrivez ici le processus de gestion des archives (versement, stockage, consultation, etc.) relevant de votre responsabilité. Précisez les rôles en matière d'archivage (service producteur, service versant, etc.) et la politique d'archivage. *Indiquez si les données sont susceptibles de relever des archives publiques.*

Sécurité des documents papier

Si des documents papiers contenant des données sont utilisés dans le cadre du traitement, indiquez ici comment ils sont imprimés, stockés, détruits et échangés.

3.1.2 Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre

Les mesures suivantes relèvent généralement de la sécurité de l'ensemble de l'organisme. Elles peuvent notamment être formalisées dans une politique de sécurité des systèmes d'information (PSSI) ou équivalent.

Sécurité de l'exploitation

*Décrivez ici comment les **mises à jour des logiciels** (systèmes d'exploitation, applications, etc.) et l'application des correctifs de sécurité sont réalisées.*

Note : penser aux possibilités de mettre à jour l'appareil.

Gestion des postes de travail et lutte contre les logiciels malveillants

Détaillez ici les mesures mises en œuvre sur les postes de travail (verrouillage automatique, pare-feu, etc.) et précisez si un antivirus est installé et régulièrement mis à jour sur tous les postes.

Sécurité des sites web

Indiquez ici si les "Recommandations pour la sécurisation des sites web" de l'ANSSI sont mises en œuvre.

Sauvegardes

Indiquez ici comment les sauvegardes sont gérées. Précisez si elles sont stockées dans un endroit sûr.

Maintenance

Décrivez ici comment est gérée la maintenance physique des équipements, et précisez si elle est sous-traitée.

Indiquez si la maintenance à distance des applications est autorisée, et suivant quelles modalités.

Précisez si les matériels défectueux sont gérés spécifiquement.

Sécurité des canaux informatiques (réseaux)

Indiquez ici sur quel type de réseau le traitement est mis en œuvre (isolé, privé, ou Internet).
Précisez quels système de pare-feu, sondes de détection d'intrusion, ou autres dispositifs actifs ou passifs sont chargés d'assurer la sécurité du réseau.

Surveillance

Indiquez ici si une surveillance en temps réel du réseau local est mise en œuvre et avec quels moyens.
Indiquez si un contrôle des configurations matérielles et logicielles est effectué et par quels moyens.

Contrôle d'accès physique

Indiquez ici la manière dont est réalisé le contrôle d'accès physique aux locaux hébergeant le traitement (zonage, accompagnement des visiteurs, port de badge, portes verrouillées, etc.).
Indiquez s'il existe des moyens d'alerte en cas d'effraction.

Sécurité des matériels

*Indiquez ici les mesures de **sécurité physique des serveurs et des postes clients** (stockage sécurisé, câbles de sécurité, filtres de confidentialité, effacement sécurisé avant mise au rebut, etc.).*

Éloignement des sources de risques

*Indiquez ici si la zone d'implantation est sujette à des **sinistres environnementaux** (zone inondable, proximité d'industries chimiques, zone sismique ou volcanique, etc.).*
*Précisez si la zone contient des **produits dangereux**.*

Protection contre les sources de risques non humaines

*Décrivez ici les moyens de prévention, de détection et de lutte contre l'**incendie**.*
*Le cas échéant, indiquez les moyens de prévention de **dégâts des eaux**.*
*Précisez également les moyens de surveillance et de secours de l'**alimentation électrique**.*

3.1.3 Mesures organisationnelles (gouvernance)

Organisation

*Indiquez si les **rôles et responsabilités** en matière de protection des données sont définis.*
Précisez si une personne est chargée de la mise en application des lois et règlements touchant à la protection de la vie privée.
*Précisez s'il existe un **comité de suivi** (ou équivalent) chargé des orientations et du suivi des actions concernant la protection de la vie privée.*

Politique (gestion des règles)

*Indiquez ici s'il existe une **charte informatique** (ou équivalent) traitant de la protection des données et de la bonne utilisation des moyens informatiques.*

Gestion des risques

Indiquez ici si les risques que les traitements font peser sur la vie privée des personnes concernées sont étudiés pour les nouveaux traitements, si c'est systématique ou non, et le cas échéant, selon quelle méthode.
Précisez s'il existe, au niveau de l'organisme, une cartographie des risques sur la vie privée.

Gestion des projets

*Indiquez ici si les **tests** des dispositifs sont réalisés sur des données fictives/anonymes.*

Gestion des incidents et des violations de données

*Indiquez ici si les **incidents** informatiques font l'objet d'une gestion documentée et testée.*

Gestion des personnels

Indiquez ici les mesures de sensibilisation prises à l'arrivée d'une personne dans sa fonction.

Indiquez les mesures prises au départ des personnes accédant aux données.

Relations avec les tiers

*Indiquez ici, pour les **sous-traitants** amenés à avoir accès aux données, les modalités et les mesures de sécurité mises en œuvre pour ces accès.*

Supervision

Indiquez ici si l'effectivité et l'adéquation des mesures touchant à la vie privée sont contrôlées.

3.1.4 Évaluation des mesures de sécurité

Vous trouverez ci-dessous un tableau permettant, pour chacune des mesures de sécurité recommandées par la CNIL, de résumer la manière dont elle est mise en œuvre ou de justifier pourquoi elle ne l'est pas.

Les deux dernières colonnes sont destinées à l'évaluateur :

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures respectent les bonnes pratiques recommandées par la CNIL.

→ Mesures correctives :

Le cas échéant, il indiquera les mesures complémentaires qui seraient nécessaires.

Mesures portant spécifiquement sur les données du traitement	Mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Chiffrement			
Anonymisation			
Cloisonnement des données (par rapport au reste du système d'information)			
Contrôle des accès logiques			
Traçabilité (journalisation)			
Contrôle d'intégrité			
Archivage			
Sécurité des documents papier			
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	**Mise en œuvre ou justification sinon**	**Acceptable / améliorable ?**	**Mesures correctives**
Sécurité de l'exploitation			
Gestion des postes de travail et lutte contre les logiciels malveillants			
Sécurité des sites web			
Sauvegardes			
Maintenance			
Sécurité des canaux informatiques (réseaux)			
Surveillance			
Contrôle d'accès physique			
Sécurité des matériels			
Éloignement des sources de risques			
Protection contre les sources de risques non humaines			

Mesures organisationnelles (gouvernance)	Mise en œuvre ou justification sinon	Acceptable / améliorable ?	Mesures correctives
Organisation			
Politique (gestion des règles)			
Gestion des risques			
Gestion des projets			
Gestion des incidents et des violations de données			
Gestion des personnels			
Relations avec les tiers			
Supervision			

3.2 Appréciation des risques : les atteintes potentielles à la vie privée

Généralement réalisée par la maîtrise d'ouvrage, puis évaluée par une personne en charge de la sécurité de l'information.

Objectif : obtenir une bonne compréhension des causes et conséquences des risques.

- Pour chaque événement redouté (un accès illégitime à des données[46], une modification non désirée de données[47], et une disparition de données[48]) :
  - déterminer les **impacts** potentiels[49] sur la vie privée des personnes concernées s'ils survenaient[50] ;
  - estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
  - Identifier les **menaces**[51] sur les supports des données qui pourraient mener à cet événement redouté[52] et les **sources de risques**[53] qui pourraient en être à l'origine ;
  - estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier ;
- Déterminer si les risques ainsi identifiés[54] peuvent être jugé acceptables compte tenu des mesures existantes ou prévues (déjà engagées).
- Dans la négative, proposer des mesures complémentaires et réévaluer le niveau de chacun des risques en tenant compte de celles-ci, afin de déterminer les risques résiduels[55].

Attention : les mesures existantes ou prévues (déjà engagées) étant prises en compte dans l'appréciation des risques, il est nécessaire, avant d'aborder la présente partie 3.2, que les mesures identifiées au §2 (juridiques) et au §3.1 (sécurité) aient été évaluées afin de s'assurer que leur liste est complète et conforme à la réalité du terrain.

Attention : les éventuelles mesures correctives proposées par l'évaluateur au §2.3 et au §3.1.4 devront, quant à elles, être prises en compte lors du calcul des risques résiduels au §3.2.1, au §3.2.2 et au §3.2.3, en même temps que les mesures correctives spécifiques à chacun des risques.

L'ensemble des mesures correctives sera repris dans le plan d'action au §4.1.

[46] Elles sont connues de personnes non autorisées (atteinte à la confidentialité des données).
[47] Elles ne sont plus intègres ou sont changées (atteinte à l'intégrité des données).
[48] Elles ne sont pas ou plus disponibles (atteinte à la disponibilité des données).
[49] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[50] Répondre à la question « Que craint-on qu'il arrive aux personnes concernées ? ».
[51] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.
[52] Répondre à la question « Comment cela pourrait-il arriver ? ».
[53] Voir l'annexe 2 – Sources de risques.
[54] Un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne.
[55] Risques qui subsistent après application des mesures.

3.2.1 Accès illégitime à des données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risque	Principales sources de risques[56]	Principales menaces[57]	Principaux impacts potentiels[58]	Principales mesures réduisant la gravité et la vraisemblance[59]	Gravité[60]	Vraisemblance[61]
Accès illégitime à des données	Entourage malintentionné Voisin malintentionné Employé malintentionné Société tierce autorisée Attaquant ciblant un utilisateur ou une des sociétés	Consultation/vol des données sur le serveur Usurpation d'un compte (via un *smartphone*) Récupération d'un appareil mis au rebut	Conséquences d'une communication d'informations potentiellement sensibles (discrimination, menaces, agressions, perte d'emploi, perte d'accès à des services, *etc.*) *Phishing* Publicité ciblée	Minimisation Durées de conservation Contrôle d'accès logique des utilisateurs Chiffrement de flux (SSL) Authentification des équipements *Cloud* privé Contrôle d'accès logique des utilisateurs Habilitation des employés Journalisation des accès Audits des journaux Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées	Importante	Maximale

Décrivez ici quelques scénarios représentatifs du risque d'accès illégitime aux données, en reprenant les sources, les menaces et les impacts.

Vous trouverez ci-dessous une illustration basée sur notre exemple de jouet fictif :

[56] Sources pertinentes pour ce risque, parmi celles identifiés dans le contexte du traitement (cf. annexe 2 – Sources de risques).
[57] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.
[58] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[59] Mesures parmi celles identifiées au §2 (juridiques) et au §3.1 (sécurité).
[60] Voir l'annexe 3 – Échelle de gravité et exemples d'impacts.
[61] Voir l'annexe 4 – Échelle de vraisemblance et exemples de menaces.

Des données pourraient être volées par un employé agissant par appât du gain ou malveillance, consultées par l'entourage usurpant le compte via le smartphone, ou récupérées sur un matériel mis au rebut par le voisinage ou un attaquant dans le but de caractériser une situation relevant de la vie privée des personnes.

Évaluation des risques résiduels

→ *Acceptable / améliorable ?*

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ *Mesures correctives :*

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ *Risques résiduels :*

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

Attention : une mesure complémentaire prise pour traiter un des risques peut également avoir un effet, positif ou négatif, sur les autres risques.

Vous trouverez ci-dessous une illustration basée sur notre exemple de jouet fictif :

→ *Améliorable :*

Les mesures prévues ne réduisent pas suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ *Mesures correctives :*

- mettre en œuvre des mesures de chiffrement des données stockées en base ;
- préciser à l'utilisateur les bonnes pratiques à suivre lors de la mise au rebut des matériels ;
- mettre en place une charte d'utilisation des moyens informatiques et un engagement de confidentialité pour les employés.

→ *Risques résiduels :*

Des données pourraient être consultées par l'entourage usurpant le compte via le smartphone.

***Gravité** : Importante* ***Vraisemblance** : Négligeable*

3.2.2 Modification non désirée de données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque. Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risques	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Modification non désirée de données	Utilisateur ou entourage, négligent ou malintentionné Voisin malintentionné Employé négligent ou malintentionné Attaquant ciblant une des sociétés	Altération des données sur le serveur	Usurpation d'identité Détérioration de la qualité du service	Sauvegarde du serveur *cloud* Chiffrement de flux (SSL) Authentification des équipements *Cloud* privé Contrôle d'accès logique des utilisateurs Habilitation des employés Journalisation des accès Audits des journaux Notification de la violation aux personnes concernées et prescription de mesures préventives adaptées	Limitée	Limitée

Décrivez ici quelques scénarios représentatifs du risque de modification non désirée de données, en reprenant les sources, les menaces et les impacts.

Évaluation des risques résiduels

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ Mesures correctives :

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ Risques résiduels :

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

3.2.3 Disparition de données

Évaluation du risque

Vous trouverez ci-dessous un tableau permettant de consigner le résultat de l'analyse de ce risque. Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Risques	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Disparition de données	Utilisateur ou entourage, négligent ou malintentionné Employé négligent ou malintentionné Attaquant ciblant un utilisateur ou une des sociétés Sinistre chez une des sociétés	Suppression de données (via l'application ou le serveur) Détérioration de serveurs Dégradation physique de l'appareil	Nécessité de recréer un compte d'utilisation Perte de l'historique et de la personnalisation du service Détérioration de la qualité du service	Sauvegarde du serveur *cloud* *Cloud* privé Protection physique des serveurs *cloud* Maintenance Conservation locale et temporaire des données Contrôle d'accès logique des utilisateurs Habilitation des employés Authentification forte des employés Journalisation des accès Garantie pour l'appareil	Limitée	Limitée

Décrivez ici quelques scénarios représentatifs du risque de disparition de données, en reprenant les sources, les menaces et les impacts.

Évaluation des risques résiduels

→ Acceptable / améliorable ?

L'évaluateur devra estimer si les mesures existantes ou prévues (déjà engagées) réduisent suffisamment ce risque pour qu'il puisse être jugé acceptable.

→ Mesures correctives :

Le cas échéant, il indiquera ici les mesures complémentaires qui seraient nécessaires.

→ Risques résiduels :

L'évaluateur indiquera ici le risque demeurant pour le traitement après la mise en œuvre des mesures complémentaires ci-dessus, en estimant la gravité et la vraisemblance compte tenu de ces mesures.

Gravité : ***Vraisemblance :***

4 Validation du PIA

Généralement réalisée par le responsable de traitement, avec l'aide d'une personne en charge des aspects « Informatique et libertés », notamment le Délégué à la protection des données si désigné.

Objectif : Décider d'accepter ou non le PIA au regard des résultats de l'étude.

4.1 Préparation des éléments utiles à la validation

- Consolider et mettre en forme les résultats de l'étude :
  1. élaborer une représentation visuelle des **mesures choisies pour respecter les principes fondamentaux,** en fonction de leur conformité au [RGPD] (ex : à améliorer, ou jugé comme conforme) ;
  2. élaborer une représentation visuelle des **mesures choisies pour contribuer à la sécurité des données,** en fonction de leur conformité aux bonnes pratiques de sécurité (ex : à améliorer, ou jugé comme conforme) ;
  3. élaborer une cartographie visuelle des **risques** (le cas échéant, initiaux et résiduels[62]) en fonction de leur gravité et vraisemblance ;
  4. élaborer un **plan d'action** à partir des mesures complémentaires identifiées lors des étapes précédentes : pour chaque mesure, déterminer au moins le responsable de sa mise en œuvre, son coût (financier ou en termes de charge) et son échéance prévisionnelle.

- Formaliser la prise en compte des parties prenantes :
  1. le **conseil de la personne en charge des aspects « Informatique et libertés »**[63];
  2. l'**avis des personnes concernées ou de leurs représentants**[64].

Note : Les zones permettant de consigner l'évaluation des mesures et des risques sont insérées directement au sein des parties précédentes, au plus près des éléments à évaluer.

Toutes les parties doivent avoir été évaluées avant de statuer sur la validation du PIA.

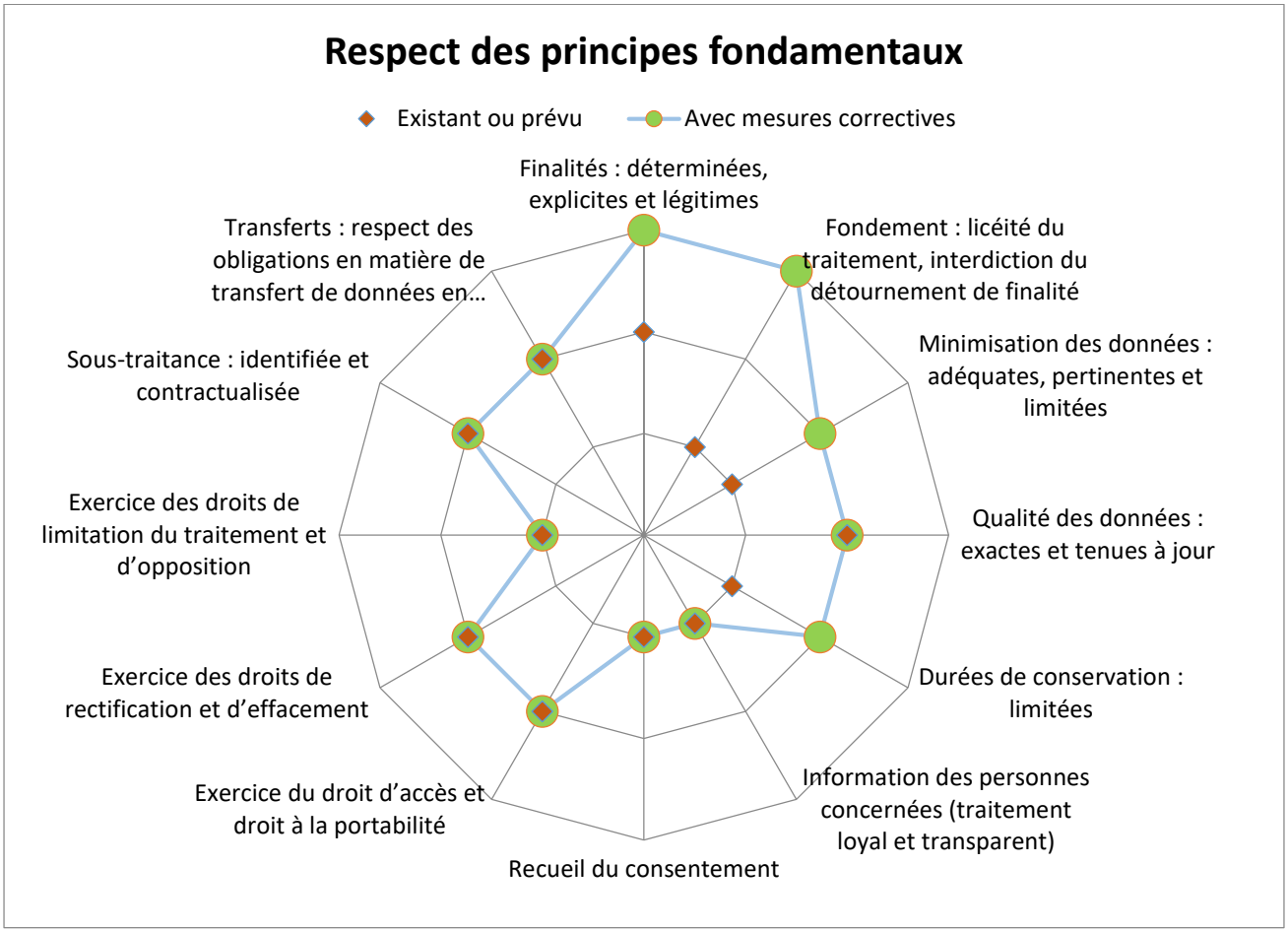
[62] Risques qui subsistent après application des mesures.
[63] Voir article 35 (2) du [RGPD]
[64] Voir article 35 (9) du [RGPD]

4.1.1 Cartographie du respect des principes fondamentaux

Vous trouverez ci-dessous un graphique pour représenter les mesures de respect des principes fondamentaux, en attribuant à chacune une valeur de conformité selon son évaluation au §2.3.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, le respect des principes fondamentaux pourrait être représenté comme suit :



Échelle du graphe :

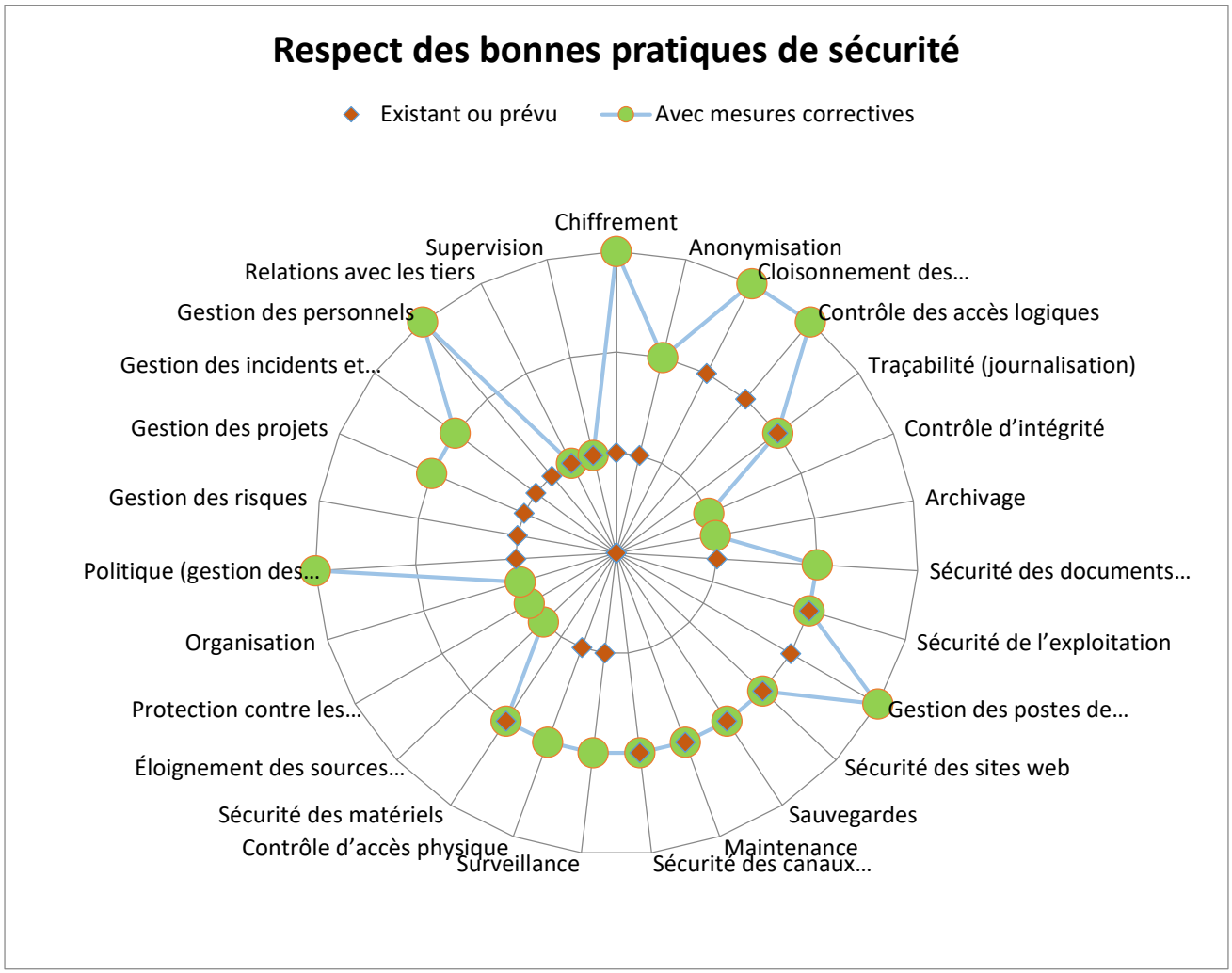
0. Non applicable
1. Améliorable
2. Acceptable
3. Bonnes pratiques

4.1.2 Cartographie du respect des bonnes pratiques de sécurité

Vous trouverez ci-dessous un graphique pour représenter les bonnes pratiques de sécurité, en attribuant à chacune une valeur de conformité selon son évaluation au §3.1.4.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, le respect des bonnes pratiques de sécurité pourrait être représenté comme suit :



Échelle du graphe :

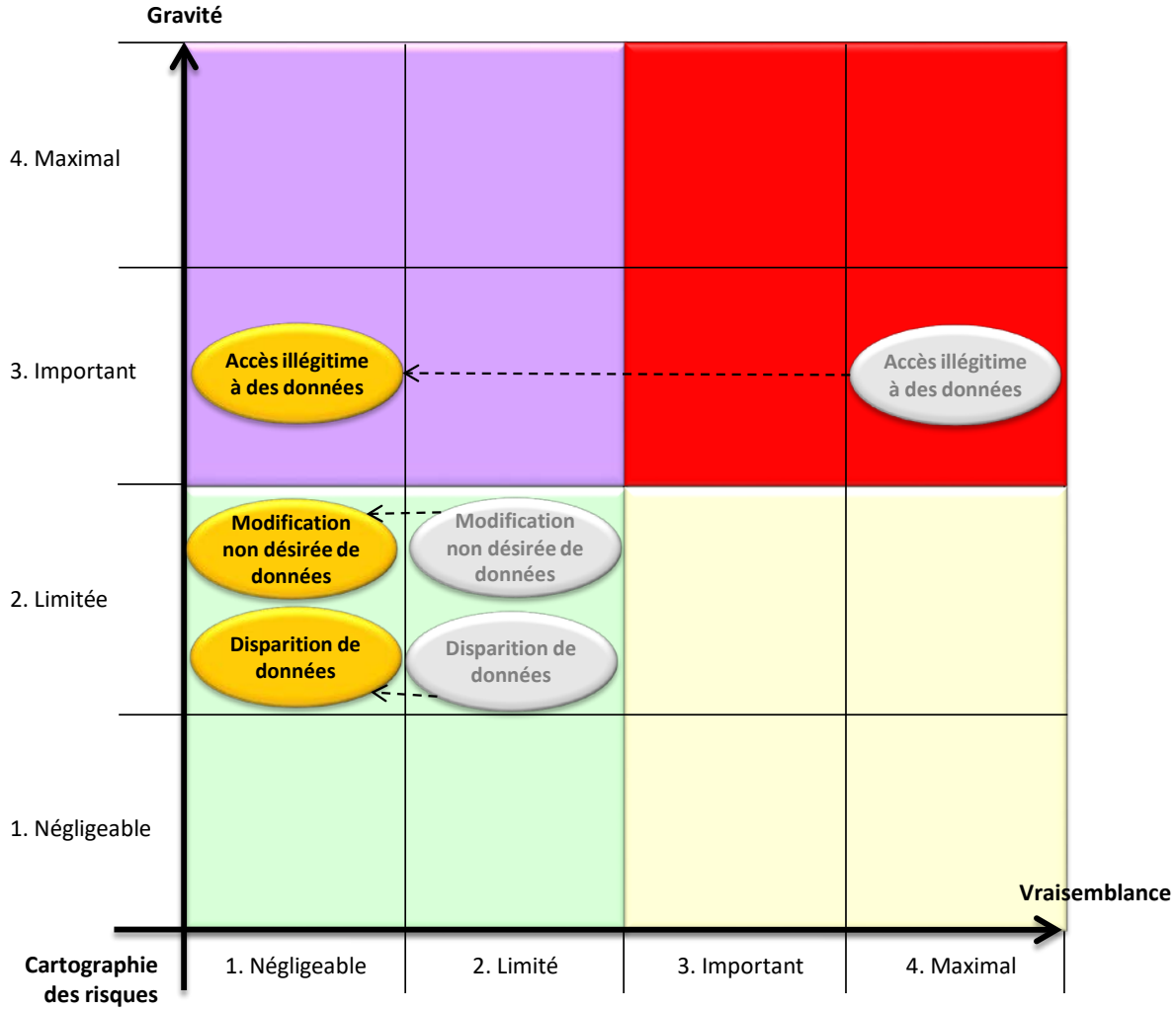
0. Non applicable
1. Améliorable
2. Acceptable
3. Bonnes pratiques

4.1.3 Cartographie des risques

Vous trouverez ci-dessous un graphique pour représenter les risques engendrés par le traitement et les risques résiduels compte tenu de l'ensemble des mesures correctives du plan d'action au §4.1.

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Si les mesures complémentaires sont correctement mises en œuvre, les risques résiduels devraient être les suivants :



4.1.4 Plan d'action : détail des mesures complémentaires prévues

Vous trouverez ci-dessous un tableau pour regrouper l'ensemble des mesures correctives proposées par l'évaluateur au §2.3, §3.1.4, §3.2.1, §3.2.2 et §3.2.3, et ainsi constituer un plan d'action en indiquant pour chaque action son responsable, son terme, sa difficulté, son coût et son état d'avancement (cf. annexe 5 – Échelles pour le plan d'action).

Pour illustrer son utilisation, il est renseigné avec les éléments de notre exemple de jouet fictif.

Mesures complémentaires demandées	Responsable	Terme	Difficulté	Coût	Avancement
Préciser à l'utilisateur les bonnes pratiques à suivre lors de la mise au rebut des matériels	Service clients et RSSI	Mois	Faible	Nul	Non démarré
Mettre en place une charte d'utilisation des moyens informatiques à destination des employés	Service juridique et RSSI	Mois	Faible	Nul	En cours
Mettre en place un engagement de confidentialité des employés	Service juridique et RSSI	Mois	Faible	Nul	Non démarré
Mettre en œuvre des mesures de chiffrement des données stockées en base	MOE et RSSI	Trimestre	Moyenne	Moyen	Non démarré

Attention : toutes les mesures spécifiées dans le plan d'action devront être formalisées, mises en place, contrôlées de manière régulière et améliorées de manière continue.

4.1.5 Conseil de la personne en charge des aspects « Informatique et libertés »[65]

Vous trouverez ci-dessous une zone pour consigner l'avis général de la personne en charge des aspects « Informatique et libertés », avant validation.

Note : cet avis peut être défavorable à la mise en œuvre du traitement, sans pour autant contraindre la décision du responsable de traitement.

Le jj/mm/aaaa, le Délégué à la Protection des Données de la société X a rendu l'avis suivant concernant la conformité du traitement et de l'étude PIA réalisée :

[Signature]

[65] Voir l'article 35 (2) du [RGPD].

4.1.6 Avis des personnes concernées ou de leurs représentants[66]

Vous trouverez ci-dessous une zone pour consigner l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu.

Attention[67] : le responsable de traitement doit demander l'avis des personnes concernées ou de leurs représentants, le cas échéant.

Cet avis peut être recueilli par divers moyens, selon le contexte (étude interne ou externe concernant la finalité et les moyens du traitement, question aux représentants du personnel ou aux syndicats, enquête auprès des futurs clients du responsable de traitement.

Si le responsable de traitement décide de passer outre l'avis des personnes concernées, il doit consigner la justification de sa décision.

Si le responsable de traitement considère que recueillir l'avis des personnes concernées n'est pas pertinent, il doit également en consigner la justification.

Les personnes concernées [ont/n'ont pas été] consultées [et ont émis l'avis suivant sur la conformité du traitement au vu de l'étude réalisée] :

Justification de la décision du responsable de traitement :

[66] Voir l'article 35 (9) du [RGPD].
[67] Voir les lignes directrices du G29 sur les PIA (en anglais).

4.2 Validation formelle du PIA

- Décider de l'acceptabilité des mesures choisies, des risques résiduels et du plan d'action, de manière argumentée, au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être :
  - validé ;
  - à améliorer (expliquer en quoi) ;
  - refusé (ainsi que le traitement considéré).

- Le cas échéant, revoir les étapes précédentes pour que le PIA puisse être validé[68].

Note : cette décision ne préjuge en rien de l'évaluation de conformité qui peut être faite, le cas échéant, par l'autorité de protection des données (en France, la CNIL), par exemple dans le cadre de formalités préalables ou de contrôles.

Vous trouverez ci-dessous un modèle de validation formelle du PIA, illustré avec les éléments de notre exemple de jouet fictif.

Le jj/mm/aaaa, le directeur général de la société X valide le PIA du traitement de jouet connecté, au vu de l'étude réalisée, en sa qualité de responsable du traitement.

Le traitement a pour finalité de fournir une interactivité à l'enfant, à travers la possibilité de dialogue avec le jouet (questions/réponses en langage naturel par reconnaissance vocale), de permettre à l'enfant de communiquer en ligne (envoi de messages vocaux, de textes et de photos) avec ses amis et/ou ses parents et de remonter des informations aux parents (dispositif de surveillance).

Les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques sur la vie privée des personnes concernées sont en effet jugées acceptables au regard de cet enjeu. La mise en œuvre des mesures complémentaires devra toutefois être démontrée, ainsi que l'amélioration continue du PIA.

[Signature]

[68] Voir notamment l'annexe 6 – Typologie d'objectifs pour traiter les risques.

Annexes

1. Mesures de minimisation des données

Mesures de minimisation	Description
Filtrage et retrait	Lors de l'importation de données, différents types de métadonnées (par exemple, des données EXIF attachées avec un fichier d'image) peuvent être involontairement collectés. Ces métadonnées doivent être identifiées et éliminées si elles ne sont pas nécessaires aux finalités spécifiées.
Réduction de la sensibilité par transformation	Après réception de données sensibles, faisant partie d'un lot d'informations générales ou transmises à des fins statistiques uniquement, celles-ci peuvent être converties en une forme moins sensible ou pseudonymisée. Par exemple, si le système collecte l'adresse IP pour déterminer l'emplacement de l'utilisateur dans un but statistique, l'adresse IP peut être supprimées après déduction de la ville ou du quartier. Si le système reçoit des données vidéo à partir de caméras de surveillance, il peut reconnaître les personnes debout ou en mouvement dans la scène et les flouter. Si le système est un compteur intelligent, il peut agréger l'utilisation de l'énergie sur une certaine période, sans l'enregistrer en temps réel.
Réduction du caractère identifiant des données	Le système peut faire en sorte que : 1) l'utilisateur peut utiliser une ressource ou un service sans risque de divulguer son identité (données anonymes) 2) l'utilisateur peut utiliser une ressource ou un service sans divulguer son identité, mais reste identifiable et responsable de cette utilisation (données pseudonymes) 3) l'utilisateur peut faire de multiples utilisations des ressources ou des services sans risque que ces utilisations puissent être reliées ensemble (données non corrélables) 4) l'utilisateur peut utiliser une ressource ou un service sans risque que d'autres, en particulier des tiers, puissent être en mesure d'observer que la ressource ou le service est utilisé (non-observabilité) Le choix d'une méthode de la liste ci-dessus doit dépendre des menaces identifiées. Pour certains types de menaces sur la vie privée, la pseudonymisation sera plus appropriée que l'anonymisation (par exemple, s'il y a un besoin de traçabilité). En outre, certaines menaces sur la vie privée seront traitées par une combinaison de plusieurs méthodes.
Réduction de l'accumulation de données	Le système peut être structuré en parties indépendantes avec des fonctions de contrôle d'accès distinctes. Les données peuvent également être réparties entre ces sous-systèmes indépendants et contrôlées par chaque sous-système en utilisant différents mécanismes de contrôle d'accès. Si un sous-système est compromis, les impacts sur l'ensemble des données peuvent ainsi être réduits.
Restriction de l'accès aux données	Le système peut limiter l'accès aux données selon le principe du « besoin d'en connaître ». Le système peut séparer les données sensibles et appliquer des politiques de contrôle d'accès spécifiques. Le système peut aussi chiffrer les données sensibles pour protéger leur confidentialité lors de la transmission et du stockage. L'accès aux fichiers cachés temporaires qui sont produits au cours du traitement des données devrait également être protégé.

2. Sources de risques

À titre d'illustration, le tableau suivant décrit les sources de risques et leurs capacités, pertinentes dans le contexte de notre exemple de jouet fictif.

Types de sources de risques	Sources de risques pertinentes	Description des capacités	Description des motivations	Décision
Sources humaines internes agissant accidentellement ou de manière délibérée	**Employé négligent ou malintentionné**	Proximité du système, compétences, privilèges et temps disponible potentiellement élevés, possible manque de formation et de sensibilisation	Maladresse, erreur, négligence Vengeance, volonté d'alerter, malveillance Appât du gain, espionnage,	Retenu
	Utilisateur ou entourage, négligent ou malintentionné	Accès direct à l'appareil et à l'application	Maladresse, erreur, négligence Jeu, malveillance Vengeance, espionnage	Retenu
Sources humaines externes agissant de manière délibérée	**Voisin malintentionné**	Proximité physique permettant de s'insérer dans les communications de l'appareil	Jeu, nuisance, malveillance Vengeance, espionnage	Retenu
	Attaquant ciblant un utilisateur	Connaissance de l'utilisateur et de certaines des informations le concernant	Jeu, nuisance, malveillance Vengeance, espionnage	Retenu
	Attaquant ciblant une des sociétés	Connaissance des sociétés pouvant permettre d'attenter à leur image	Vengeance, volonté d'alerter, malveillance Appât du gain, espionnage	Retenu
	Société tierce autorisée	Accès privilégiés pouvant être utilisés pour accéder illégitimement à des informations	Appât du gain, volonté de disposer de beaucoup de données et de les exploiter	Retenu
Sources humaines externes agissant accidentellement	**Voisin ignorant**	Proximité physique permettant d'émettre sur le canal de communication de l'appareil	Ignorance	Non retenu
Sources non humaines	**Incident ou sinistre chez l'utilisateur** (coupure de courant, incendie, inondation, *etc.*)	Divers		Non retenu
	Sinistre chez une des sociétés (coupure de courant, incendie, inondation, *etc.*)	Divers		Retenu

3. Échelle de gravité et exemples d'impacts

L'échelle suivante peut être utilisée pour estimer la gravité des événements redoutés (**attention : ce ne sont que des exemples, qui peuvent être très différents selon le contexte**) :

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[69]	Exemples d'impacts matériels[70]	Exemples d'impacts moraux[71]
1. Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) Maux de tête passagers	Perte de temps pour réitérer des démarches ou pour attendre de les réaliser Réception de courriers non sollicités (ex. : *spams*) Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) Publicité ciblée pour des produits de consommation courants	Simple contrariété par rapport à l'information reçue ou demandée Peur de perdre le contrôle de ses données Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) Perte de temps pour paramétrer ses données Non respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)
2. Limitée	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Affection physique mineure (ex. : maladie bénigne suite au non respect de contre-indications) Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) Diffamation donnant lieu à des représailles physiques ou psychiques	Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement Refus d'accès à des services administratifs ou prestations commerciales Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) Promotion professionnelle manquée Compte à des services en ligne bloqué (ex. : jeux, administration) Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées Élévation de coûts (ex. : augmentation du prix d'assurance)	Refus de continuer à utiliser les systèmes d'information (*whistleblowing*, réseaux sociaux) Affection psychologique mineure mais objective (diffamation, réputation) Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) Sentiment d'atteinte à la vie privée sans préjudice irrémédiable Intimidation sur les réseaux sociaux

[69] Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique.
[70] Perte subie ou gain manqué concernant le patrimoine des personnes.
[71] Souffrance physique ou morale, préjudice esthétique ou d'agrément.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels[69]	Exemples d'impacts matériels[70]	Exemples d'impacts moraux[71]
			Données non mises à jour (ex. : poste antérieurement occupé) Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) Profilage imprécis ou abusif	
3. Importante	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non respect de contre-indications) Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	Détournements d'argent non indemnisé Difficultés financières non temporaires (ex. : obligation de contracter un prêt) Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) Interdiction bancaire Dégradation de biens Perte de logement Perte d'emploi Séparation ou divorce Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage - *phishing*) Bloqué à l'étranger Perte de données clientèle	Affection psychologique grave (ex. : dépression, développement d'une phobie) Sentiment d'atteinte à la vie privée et de préjudice irrémédiable Sentiment de vulnérabilité à la suite d'une assignation en justice Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) Victime de chantage *Cyberbullying* et harcèlement moral
4. Maximale	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Affection physique de longue durée ou permanente (ex. : suite au non respect d'une contre-indication) Décès (ex. : meurtre, suicide, accident mortel) Altération définitive de l'intégrité physique	Péril financier Dettes importantes Impossibilité de travailler Impossibilité de se reloger Perte de preuves dans le cadre d'un contentieux Perte d'accès à une infrastructure vitale (eau, électricité)	Affection psychologique de longue durée ou permanente Sanction pénale Enlèvement Perte de lien familial Impossibilité d'ester en justice Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

4. Échelle de vraisemblance et exemples de menaces

L'échelle suivante peut être utilisée pour estimer la vraisemblance des menaces :

1. Négligeable : il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité : il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important : il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal : il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

L'action des sources de risques sur les supports constitue une menace. Les supports peuvent être :

- utilisés de manière inadaptée : les supports sont utilisés hors de leur cadre d'utilisation prévu, voire détournés, sans être modifiés ni endommagés ;
- observés : les supports sont observés ou espionnés sans être endommagés ;
- surchargés : les limites de fonctionnement des supports sont dépassées, ils sont surchargés, surexploités ou utilisés dans des conditions ne leur permettant pas de fonctionner correctement ;
- détériorés : les supports sont endommagés, partiellement ou totalement ;
- modifiés : les supports sont transformés ;
- perdus : les supports sont perdus, volés, vendus ou donnés, de telle sorte qu'il n'est plus possible d'exercer les droits de propriété.

Les menaces génériques qui suivent sont conçues pour être exhaustives, indépendantes et appliquées aux spécificités de la protection de la vie privée.

Menaces pouvant mener à un accès illégitime aux DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Matériels	Utilisés de manière inadaptée	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles, le disque dur contenant les informations est utilisé pour une fin non prévue (par exemple pour transporter d'autres données chez un prestataire, pour transférer d'autres données d'une base de données à une autre, etc.)	Utilisable en dehors de l'usage prévu, disproportion entre le dimensionnement des matériels et le dimensionnement nécessaire (par exemple : disque dur de plusieurs To pour stocker quelques Go de données)
Matériels	Observés	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance	Permet d'observer des données interprétables, émet des signaux compromettants
Matériels	Modifiés	Piégeage par un *keylogger*, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Matériels	Perdus	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique	Petite taille, attractif (valeur marchande)
Logiciels	Utilisés de manière inadaptée	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
Logiciels	Observés	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source
Logiciels	Modifiés	Piégeage par un *keylogger* logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre lors d'une mise à jour, d'une opération de maintenance ou d'une installation (des bouts de codes ou applications sont installés ou remplacés)	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
Canaux informatiques	Observés	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables
Personnes	Observées	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle	Peu discret (loquace, sans réserve), routinier (habitudes facilitant l'espionnage récurrent)
Personnes	Détournées	Influence (hameçonnage, filoutage, ingénierie sociale, corruption), pression (chantage, harcèlement moral)	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté), manipulable (vulnérable aux pressions sur soi ou son entourage)
Personnes	Perdues	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
Documents papier	Observés	Lecture, photocopie, photographie	Permet d'observer des données interprétables
Documents papier	Perdus	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut	Portable
Canaux papier	Observés	Lecture de parapheurs en circulation, reproduction de documents en transit	Observable

Menaces pouvant mener à une modification non désirées des DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Matériels	Modifiés	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
Logiciels	Utilisés de manière inadaptée	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
Canaux informatiques	Utilisés de manière inadaptée	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds)
Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement
Personnes	Détournées	Influence (rumeur, désinformation)	Influençable (naïf, crédule, obtus)
Documents papier	Modifiés	Modification de chiffres dans un dossier, remplacement d'un document par un faux	Falsifiable (support papier au contenu modifiable)
Canaux papier	Modifiés	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier

Menaces pouvant mener à une disparition des DCP

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Matériels	Utilisés de manière inadaptée	Stockage de fichiers personnels, utilisation à des fins personnelles	Utilisable en dehors de l'usage prévu
Matériels	Surchargés	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive, attaque par dénis de service	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension
Matériels	Modifiés	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions) via des connecteurs (ports, slots), permet de désactiver des éléments (port USB)
Matériels	Détériorés	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement) ; n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires)
Matériels	Perdus	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel, disques sous dimensionnés amenant à une multiplication des supports et à la perte de certains	Portable, attractif (valeur marchande)
Logiciels	Utilisés de manière inadaptée	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées
Logiciels	Surchargés	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues, attaque par dénis de service	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable
Logiciels	Modifiés	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre	Modifiable (améliorable, paramétrable), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes), ne fonctionne pas correctement ou conformément aux attentes
Logiciels	Détériorés	Effacement d'un exécutable en production ou de code sources, virus, bombe logique	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications)
Logiciels	Perdus	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données, arrêt des mises à jour de maintenance de sécurité par l'éditeur, faillite de l'éditeur, corruption du module de stockage contenant les numéros de licence	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne), attractif (rare, novateur, grande valeur commerciale), cessible (clause de cessibilité totale dans la licence)

Types de supports	Actions	Exemples de menaces	Exemples de vulnérabilités des supports
Canaux informatiques	Surchargés	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée)
Canaux informatiques	Détériorés	Sectionnement de câblage, mauvaise réception du réseau wifi, oxydation des câbles	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné), unique
Canaux informatiques	Perdus	Vol de câbles de transmission en cuivre	Attractif (valeur marchande des câbles), transportable (léger, dissimulable), peu visible (oubliable, insignifiant, peu remarquable)
Personnes	Surchargées	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement
Personnes	Détériorées	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique	Limites physiques, psychologiques ou mentales
Personnes	Perdues	Décès, retraite, changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel
Documents papier	Utilisés de manière inadaptée	Effacement progressif avec le temps, effacement volontaire de parties d'un texte, réutilisation des papiers pour prendre des notes sans relation avec le traitement, pour faire la liste de course, utilisation des cahiers pour faire autre chose	Modifiable (support papier au contenu effaçable, papiers thermiques non résistants aux modifications de températures)
Documents papier	Détériorés	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement), n'est pas approprié aux conditions d'utilisation
Documents papier	Perdus	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut	Portable
Canaux papier	Surchargés	Surcharge de courriers, surcharge d'un processus de validation	Existence de limites quantitatives ou qualitatives
Canaux papier	Détériorés	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève	Instable, unique
Canaux papier	Modifiés	Modification dans l'expédition des courriers, réaffectation des bureaux ou des locaux, réorganisation de circuits papier, changement de langue professionnelle	Modifiable (remplaçable)
Canaux papier	Perdus	Réorganisation supprimant un processus, disparition d'un transporteur de documents, vacance de postes	Utilité non reconnue

5. Échelles pour le plan d'action

Les échelles suivantes peuvent être utilisées pour élaborer le plan d'action et suivre sa mise en œuvre :

Critère	Niveau 1	Niveau 2	Niveau 3
Difficulté	Faible	Moyenne	Élevée
Coût financier	Nul	Moyen	Important
Terme	Année	Trimestre	Mois
Avancement	Non démarré	En cours	Terminé

6. Typologie d'objectifs pour traiter les risques

Des objectifs peuvent être fixés en fonction du niveau des risques, par exemple :

1. pour les risques dont la gravité et la vraisemblance sont élevées[72] : ces risques devraient absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;
2. pour les risques dont la gravité est élevée, mais la vraisemblance faible[73] : ces risques devraient être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ;
3. pour les risques dont la gravité est faible mais la vraisemblance élevée : ces risques devraient être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;
4. pour les risques dont la gravité et la vraisemblance sont faibles : ces risques devraient pouvoir être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Notes : Les risques peuvent généralement être réduits, transférés ou pris. Toutefois, certains risques ne peuvent l'être, notamment lorsque des données sensibles sont traitées ou quand les préjudices dont peuvent être victimes les personnes concernées sont très importants. Dans de tels cas, il pourra s'avérer nécessaire de les éviter, par exemple en ne mettant pas en œuvre tout ou partie d'un traitement.

[72] Niveaux 3. Important et 4. Maximal.
[73] Niveaux 1. Négligeable et 2. Limité.

Travail &
Données personnelles

L'accès aux locaux et le contrôle des horaires

Parce que les locaux professionnels ne sont pas ouverts à tous et que les employeurs comme les employés ont besoin de connaître les horaires effectués, les contrôles d'accès et du temps de travail existent depuis bien longtemps. Le développement des technologies facilite ces contrôles mais permet aussi de collecter bien plus d'informations sur les personnes concernées. Des limites à leur utilisation sont donc indispensables pour préserver les droits et libertés de chacun.

Dans quel but ?

L'employeur peut mettre en place des outils – y compris biométriques – de contrôle individuel de l'accès pour sécuriser :

- l'entrée dans les bâtiments,
- les locaux faisant l'objet d'une restriction de circulation.

Ces dispositifs peuvent concerner les employés comme les visiteurs.

Des dispositifs non biométriques peuvent également être utilisés pour gérer les horaires et le temps de présence des employés.

Quelles garanties pour la vie privée ?

Le système mis en place ne doit pas servir au contrôle des déplacements à l'intérieur des locaux.

Le dispositif ne doit pas entraver la liberté d'aller et venir des représentants du personnel dans l'exercice de leur mandat, ou être utilisé pour contrôler le respect de leurs heures de délégation.

Qui peut accéder aux données ?

Les informations ne sont accessibles qu'aux membres habilités des services gérant le personnel, la paie, ou la sécurité.

L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance. Ainsi, il doit prévoir des habilitations pour les accès informatiques avec une traçabilité des actions effectuées (savoir qui se connecte à quoi, quand et pour quoi faire).

Quelle durée de conservation ?

- Les données relatives aux accès doivent être supprimées **3 mois après leur enregistrement.**
- Les données utilisées pour le suivi du temps de travail, y compris les données relatives aux motifs des absences, **doivent être conservées pendant 5 ans.**

L'information des salariés

Les instances représentatives du personnel doivent être informées ou consultées avant toute décision d'installer un dispositif de contrôle des horaires ou d'accès aux locaux.

Chaque employé doit être notamment informé :
- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données issues du dispositif,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'un avenant au contrat de travail ou d'une note de service, par exemple.

L'accès aux locaux et le contrôle des horaires

Quelles sécurités ?

Pour éviter notamment que des personnes non autorisées accèdent aux données du dispositif, il est impératif de prendre des mesures de sécurité. Par exemple, l'accès au logiciel de gestion du contrôle d'accès ou des horaires doit être limité aux personnes qui ont besoin d'en connaître et se faire avec un identifiant et un mot de passe.

Il faut également impérativement prévoir :

- une politique d'habilitation,
- une sécurisation des échanges,
- une journalisation des accès aux données et des opérations, effectuées.

Une étude des risques sur la sécurité des données est également souhaitable afin de définir les mesures les mieux adaptées, notamment lorsqu'un dispositif biométrique est mis en place.

Quelles formalités ?

Les dispositifs sans biométrie

Le contrôle d'accès sans biométrie est à privilégier, dès lors qu'un système de badge est suffisant ou que les locaux ne sont pas particulièrement sensibles.

Attention, la CNIL estime que la biométrie est un moyen disproportionné de contrôle des horaires des employés.

Les dispositifs avec biométrie

Le contrôle d'accès biométrique doit faire l'objet d'une analyse d'impact sur la protection des données (PIA). Cette démarche permet d'identifier les risques associés aux données personnelles concernées par le dispositif, et à en réduire soit la vraisemblance soit la gravité.

L'aide du fournisseur, de l'intégrateur ou de l'installateur du dispositif peut être utile.

Dans ces situations, l'employeur doit privilégier le stockage du gabarit biométrique de l'employé sur un support individuel.

Si l'organisme a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre de ce dispositif.
L'employeur doit inscrire ce dispositif de contrôle dans son registre des activités de traitement de données.

Quels recours ?

En cas de difficulté, vous pouvez saisir :

- le service des plaintes de la CNIL,
- l'inspection du Travail,
- le procureur de la République.

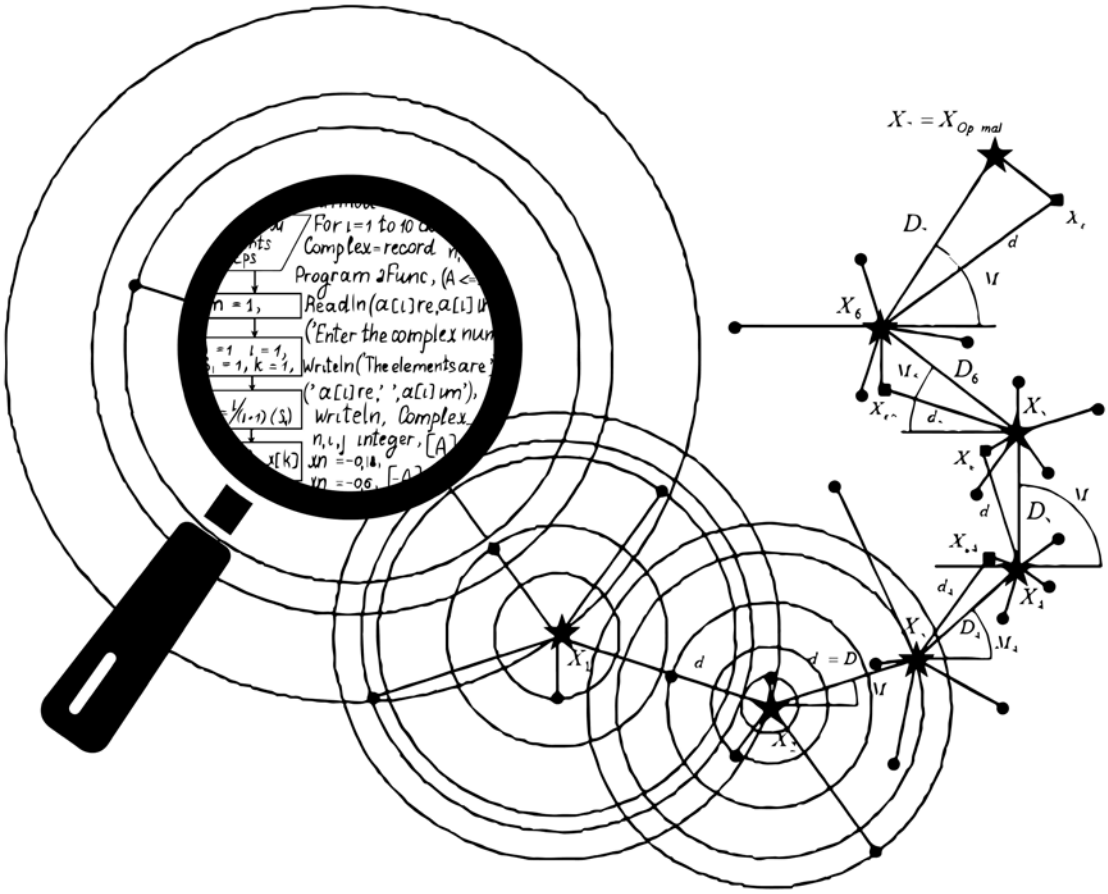
Textes de référence

- **Le code civil :**
  Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**
  Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-32 (information/consultation du comité d'entreprise)
- **Le code pénal :**
  Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Voir aussi

- Le contrôle d'accès biométrique sur les lieux de travail.
- L'analyse d'impact relative à la protection des données
- Guide de la sécurité des données personnelles

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur **www.cnil.fr**. Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.



COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ?

Les enjeux éthiques des algorithmes et de l'intelligence artificielle

SYNTHÈSE DU DÉBAT PUBLIC ANIMÉ PAR LA CNIL DANS LE CADRE DE LA MISSION DE RÉFLEXION ÉTHIQUE CONFIÉE PAR LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE

DÉCEMBRE 2017

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

et éthique numérique
les algorithmes en débat

COMMENT PERMETTRE À L'HOMME DE GARDER LA MAIN ?

Les enjeux éthiques des algorithmes et de l'intelligence artificielle

SYNTHÈSE DU DÉBAT PUBLIC ANIMÉ PAR LA CNIL DANS LE CADRE DE LA MISSION
DE RÉFLEXION ÉTHIQUE CONFIÉE PAR LA LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE

DÉCEMBRE 2017

Ce rapport a été rédigé par Victor Demiaux avec le concours de Yacine Si Abdallah.

PRÉFACE

L'intelligence artificielle est le grand mythe de notre temps. L'un annonce la destruction en masse de nos emplois, un autre l'émergence apocalyptique d'une conscience robotique hostile, un troisième la ruine d'une Europe écrasée par la concurrence. D'autres encore nourrissent plutôt le rêve d'un monde sur mesure, d'un nouvel Âge d'or d'où toute tâche ingrate ou répétitive serait bannie et déléguée à des machines ; un Eden où des outils infaillibles auraient éradiqué la maladie et le crime, voire le conflit politique, en un mot aboli le mal. Sous ses avatars tour à tour fascinants ou inquiétants, solaires ou chtoniens, l'intelligence artificielle dit sans doute plus de nos phantasmes et de nos angoisses que de ce que sera notre monde demain. À considérer l'attrait de ce type de discours eschatologiques en Europe, on en vient à penser que la technique cristallise aussi une puissance de projection dans l'avenir qui fait parfois défaut à nos imaginaires politiques.

Désamorcer ces présentations sensationnalistes des nouvelles technologies est une chose. Cela ne signifie pas pour autant que l'on ignore que l'irruption dans nos vies quotidiennes de ces assistants ou outils d'un nouveau type génère des bouleversements multiples et des défis nouveaux que nous devons relever. Préservation de l'autonomie de la décision humaine face à des machines parfois perçues comme infaillibles, détection de discriminations générées involontairement par des systèmes mouvants, sauvegarde de logiques collectives parfois érodées par la puissance de personnalisation du numérique, etc. : les enjeux ne manquent pas, aux implications déjà tangibles. Ils questionnent certains des grands pactes et des équilibres sur lesquels repose notre vie collective.

Établir de façon claire et lucide ces enjeux est le premier devoir de la puissance publique, la condition pour pouvoir proposer des réponses adaptées, pour intégrer l'innovation technologique à la construction d'une vision déterminée de notre avenir. C'était le sens de la création de la mission de réflexion sur les enjeux éthiques soulevés par les technologies numériques que la Loi pour une République numérique a confiée à la CNIL.

Comment appréhender aujourd'hui une telle mission ? Beaucoup se sont interrogés, voire ont questionné cette responsabilité nouvelle de la Commission. Comment exprimer l'éthique sur des sujets hautement complexes et évolutifs, à quel titre, selon quelles modalités ?

Réflexion sur les principes fondamentaux de conduite de la vie des hommes et des sociétés, définition d'un pacte social partagé sur un sujet complexe à un moment donné, l'éthique constitue un objet éminemment collectif, pluriel. Dans le domaine bien particulier des sciences de la vie et de la santé, la composition et la collégialité du travail du Comité Consultatif National d'Éthique répondent à cet impératif de pluralité.

Garante de principes éthiques fixés par le législateur il y a quarante ans, la CNIL a certes toute légitimité pour être le point focal de cette réflexion éthique, à l'heure où des possibilités techniques nouvelles soulèvent de nouveaux enjeux ou questionnent les équilibres antérieurs.

En revanche, il est apparu impensable qu'elle puisse se prévaloir d'un quelconque monopole sur la réflexion éthique du numérique. Sur un sujet aussi vaste et transversal, cette dernière ne saurait se concevoir en vase clos. Le numérique n'est pas un secteur, que l'on pourrait confier aux soins d'un comité d'éthique restreint à quelques membres, aussi compétents soient-ils. Il fallait innover.

C'est dans cet esprit que la CNIL a suscité une démarche collective, en animant avec l'aide de partenaires de multiples secteurs un débat public pendant plusieurs mois. L'éthique est à cet égard autant un processus d'élaboration que le résultat du processus lui-même. Nous avons ainsi fait le choix de partir des usages, des interrogations existantes et des pistes de solutions évoqués par les acteurs du débat. Plus de quarante manifestations organisées à Paris et en régions ont permis de recueillir les éléments qui ont alimenté le présent rapport et les recommandations dont il est porteur.

Un effort d'innovation était également nécessaire pour faire droit à la nécessité d'associer davantage le citoyen à l'élaboration de la réflexion publique sur un univers complexe qui modèle de plus en plus son existence et implique des choix de société fondamentaux. Un univers dont il doit être de plus en plus un co-acteur. La CNIL a ainsi organisé une journée de concertation citoyenne, à Montpellier, le 14 octobre dernier, qui a permis de joindre la voix d'une quarantaine de volontaires à la polyphonie du débat public.

Le premier bénéfice de cette démarche ouverte et décentralisée est d'avoir fait respirer le débat le plus largement possible et d'avoir participé à la montée en compétence de la société française vis-à-vis des questions soulevées par les algorithmes et par l'IA. Face à des systèmes socio-techniques de plus en plus complexes et compartimentés, face aux impacts parfois difficilement prévisibles d'artefacts en évolution constante, cloisonner le débat à quelques cercles d'initiés, c'est prendre le risque de susciter méfiance et défiance. Faire de l'ensemble de nos concitoyens des utilisateurs éclairés et critiques des technologies est au contraire un impératif tout à la fois éthique, démocratique et pragmatique. C'est aussi, pour la CNIL, prolonger l'œuvre d'accompagnement de la rencontre de la société française avec le numérique qu'elle accomplit depuis 40 ans.

À l'heure même où se définit la position française – et bientôt européenne – en matière d'intelligence artificielle, le rapport issu de ces mois de débat public contribue à poser les jalons d'un questionnement commun. Il propose un panorama des enjeux et formule un certain nombre de principes et de recommandations.

Celles-ci ont un objectif commun : permettre à la personne humaine de ne pas « perdre la main ». À l'heure de la dématérialisation généralisée, ceci paraitra peut-être décalé. Il nous semble au contraire que c'est là que réside notre défi collectif majeur. Faire en sorte que ces nouveaux outils soient à la main humaine, à son service, dans un rapport de transparence et de responsabilité.

Puissent ces réflexions alimenter celles en cours au sein des pouvoirs publics, dont celle de la mission Villani, mais aussi des différentes composantes de la société civile. Puissent-elles ainsi participer à l'élaboration d'un modèle français de gouvernance éthique de l'intelligence artificielle.

Isabelle Falque-Pierrotin
Présidente de la CNIL

SOMMAIRE

RÉSUMÉ

Ce rapport est le résultat d'un débat public animé par la CNIL. Entre janvier et octobre 2017, 60 partenaires (associations, entreprises, administrations, syndicats, etc.) ont organisé 45 manifestations dans toute la France. Il s'agissait d'identifier les sujets de préoccupations éthiques soulevés par les algorithmes et l'intelligence artificielle, ainsi que les pistes de solutions possibles.

La première partie du rapport apporte une définition pragmatique des algorithmes et de l'intelligence artificielle tout en présentant leurs principaux usages et notamment ceux d'entre eux qui retiennent aujourd'hui le plus l'attention publique. Classiquement, l'algorithme se définit ainsi comme une suite finie et non ambigüe d'instructions permettant d'aboutir à un résultat à partir de données fournies en entrée. Cette définition rend compte des multiples applications numériques qui, exécutant des programmes traduisant eux-mêmes en langage informatique un algorithme, remplissent des fonctions aussi diverses que fournir des résultats sur un moteur de recherche, proposer un diagnostic médical, conduire une voiture d'un point à un autre, détecter des suspects de fraude parmi les allocataires de prestations sociales, etc. L'intelligence artificielle désigne principalement dans le débat public contemporain une nouvelle classe d'algorithmes, paramétrés à partir de techniques dites d'apprentissage : les instructions à exécuter ne sont plus programmées explicitement par un développeur humain, elles sont en fait générées par la machine elle-même, qui « apprend » à partir des données qui lui sont fournies. Ces algorithmes d'apprentissage peuvent accomplir des tâches dont sont incapables les algorithmes classiques (reconnaître un objet donné sur de très vastes corpus d'images, par exemple). En revanche, leur logique sous-jacente reste incompréhensible et opaque y compris à ceux qui les construisent.

Le débat public a permis d'identifier 6 grandes problématiques éthiques :

- Le perfectionnement et l'autonomie croissante des artefacts techniques permettent des formes de délégations de tâches, de raisonnements et de décisions de plus en complexes et critiques à des machines. Dans ces conditions, à côté de l'augmentation de sa puissance d'agir permise par la technique, n'est-ce pas aussi son autonomie, son libre arbitre, qui peut se trouver érodé ? Le prestige et la confiance accordés à des machines jugées souvent infaillibles et « neutres » ne risquent-ils pas de générer la tentation de se décharger sur les machines de la fatigue d'exercer des responsabilités, de juger, de prendre des décisions ? Comment appréhender les formes de dilution de la responsabilité que sont susceptibles de susciter les systèmes algorithmiques, complexes et très segmentés ?

- Les algorithmes et l'intelligence artificielle peuvent susciter des biais, des discriminations, voire des formes d'exclusion. Ces phénomènes peuvent être volontaires. Mais le réel enjeu, à l'heure du développement des algorithmes d'apprentissage, est leur développement à l'insu même de l'homme. Comment y faire face ?

- L'écosystème numérique tel qu'il s'est construit avec le Web, mais également plus anciennement les techniques actuarielles, ont fortement exploité les potentialités des algorithmes en termes de personnalisation. Le profilage et la segmentation de plus en plus fine rendent bien des services à l'individu. Mais cette logique de personnalisation est également susceptible d'affecter – outre les individus – des logiques collectives essentielles à la vie de nos sociétés (pluralisme démocratique et culturel, mutualisation du risque).

- L'intelligence artificielle, dans la mesure où elle repose sur des techniques d'apprentissage, nécessite d'énormes quantités de données. Or, la législation promeut une logique de minimisation de la collecte et de la conservation de données personnelles, conforme à une conscience aigüe des risques impliqués pour les libertés individuelles et publiques de la constitution de grands fichiers. Les promesses de l'IA justifient-elles une révision de l'équilibre construit par le législateur ?

- Le choix du type de données alimentant un modèle algorithmique, leur quantité suffisante ou insuffisante, l'existence de biais dans les jeux de données servant à entraîner les algorithmes d'apprentissage constituent un enjeu majeur. S'y cristallise le besoin d'établir une attitude critique et de ne pas nourrir une confiance excessive dans la machine.

- L'autonomie croissante des machines ainsi que l'émergence de formes d'hybridation entre humains et machines (hybridation au plan d'une action assistée par des recommandations algorithmiques, mais aussi prochainement au plan physique) questionnent l'idée d'une spécificité humaine irréductible. Faut-il et est-il possible de parler au sens propre d' « éthique des algorithmes » ? Comment appréhender cette nouvelle classe d'objets que sont les robots humanoïdes, objets mais susceptibles de susciter chez l'homme des formes d'affects et d'attachement ?

La troisième partie du rapport envisage les réponses possibles formulées à l'occasion du débat public.
Elle aborde d'abord les principes susceptibles de construire une intelligence artificielle au service de l'homme. Deux principes nouveaux apparaissent comme fondateurs.

Le premier, substantiel, est le ***principe de loyauté,*** dans une version approfondie par rapport à celle initialement formulée par le Conseil d'Etat sur les plateformes. Cette version intègre en effet une dimension collective de la loyauté, celle-ci visant à ce que l'outil algorithmique ne puisse trahir sa communauté d'appartenance (consumériste ou citoyenne), qu'il traite ou non des données personnelles.

Le second, d'ordre plus méthodique, est un **principe de vigilance/réflexivité.** Il vise à répondre dans le temps au défi constitué par le caractère instable et imprévisible des algorithmes d'apprentissage. Il constitue aussi une réponse aux formes d'indifférence, de négligence et de dilution de responsabilité que peut générer le caractère très compartimenté et segmenté des systèmes algorithmiques. Il a enfin pour but de prendre en compte et de contrebalancer la forme de biais cognitif conduisant l'esprit humain à accorder une confiance excessive aux décrets des algorithmes. Il s'agit d'organiser, par des procédures et mesures concrètes, une forme de questionnement régulier, méthodique, délibératif et fécond à l'égard de ces objets techniques de la part de tous les acteurs de la chaine algorithmique, depuis le concepteur, jusqu'à l'utilisateur final, en passant par ceux qui entraînent les algorithmes.

Ces deux principes apparaissent comme fondateurs de la régulation de ces outils et assistants complexes que sont les algorithmes et l'IA. Ils en permettent l'utilisation et le développement tout en intégrant leur mise sous contrôle par la communauté.

Ils sont complétés par une ingénierie spécifique et nouvelle articulée sur deux points : l'un visant à repenser l'obligation d'intervention humaine dans la prise de décision algorithmique (article 10 de la loi Informatique et libertés) ; l'autre à organiser l'intelligibilité et la responsabilité des systèmes algorithmiques.

Ces principes font ensuite l'objet d'une déclinaison opérationnelle sous la forme de **6 recommandations** adressées tant aux pouvoirs publics qu'aux diverses composantes de la société civile (grand public, entreprises, associations, etc.) :

- Former à l'éthique tous les maillons de la « chaîne algorithmique (concepteurs, professionnels, citoyens) ;
- Rendre les systèmes algorithmiques compréhensibles en renforçant les droits existants et en organisant la médiation avec les utilisateurs ;
- Travailler le *design* des systèmes algorithmiques au service de la liberté humaine ;
- Constituer une plateforme nationale d'audit des algorithmes ;
- Encourager la recherche sur l'IA éthique et lancer une grande cause nationale participative autour d'un projet de recherche d'intérêt général ;
- Renforcer la fonction éthique au sein des entreprises.

Une démarche innovante au service de l'élaboration d'une réflexion éthique collective et pluraliste

Un débat public national sur les enjeux éthiques des algorithmes et de l'intelligence artificielle

La loi pour une République numérique de 2016 a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevés par l'évolution des technologies numériques.

La CNIL a choisi de faire porter en 2017 cette réflexion sur les algorithmes à l'heure de l'intelligence artificielle. En effet, ceux-ci occupent dans nos vies une place croissante, bien qu'invisible. Résultats de requêtes sur un moteur de recherche, ordres financiers passés par des robots sur les marchés, diagnostics médicaux automatiques, affectation des étudiants à l'Université : dans tous ces domaines, des algorithmes sont à l'œuvre. En 2016, le sujet des algorithmes s'était d'ailleurs invité de manière inédite dans le débat public et a suscité une forte attention médiatique (questions sur l'algorithme du logiciel Admission Post-Bac, recours à l'intelligence artificielle dans la stratégie électorale du candidat Trump, rôle des réseaux sociaux dans la diffusion des « fake news »).

> La réflexion éthique porte sur des choix de société décisifs. Elle ne saurait se construire indépendamment d'une prise en compte de cette dimension pluraliste et collective

La réflexion éthique porte sur des choix de société décisifs. Elle ne saurait se construire indépendamment d'une prise en compte de cette dimension pluraliste et collective. Ceci est d'autant plus vrai quand il s'agit d'un objet aussi transversal à toutes les dimensions de notre vie individuelle et sociale que les algorithmes. Il ne serait guère envisageable de rassembler en un unique comité l'ensemble des compétences et des regards nécessaire à l'examen des enjeux soulevés par les algorithmes dans des secteurs aussi divers que la santé, l'éducation, le marketing, la culture, la sécurité, etc.

Plutôt que de conduire directement sur ces sujets une réflexion centralisée, la CNIL a donc fait le choix de se positionner, d'une façon originale, en tant qu'animatrice d'un débat public national ouvert et décentralisé. À l'occasion d'un événement de lancement organisé le 23 janvier 2017, elle a ainsi appelé tous les acteurs et organismes – institutions publiques, société civile, entreprises – qui le souhaitaient à organiser un débat ou une manifestation sur le sujet, dont ils lui feraient ensuite parvenir la restitution. L'objectif a donc été de s'adresser aux acteurs de terrain pour recueillir auprès d'eux les sujets éthiques identifiés comme tels à ce jour ainsi que les pistes de solutions évoquées par les uns et par les autres.

Soixante partenaires ont souhaité répondre à l'appel lancé par la CNIL. De natures très diverses, ces acteurs relevaient de secteurs très différents. Citons, à titre d'exemples, la Ligue de l'Enseignement dans l'éducation, la Fédération Française de l'Assurance (FFA), le Ministère de la Culture (DGMIC), l'association Open Law, ou encore la CFE-CFC et FO Cadres (ressources humaines), etc. Ces 60 partenaires ont organisé 45 manifestations entre

mars et octobre 2017 dans plusieurs villes de France (mais également à l'étranger grâce à la participation de la « Future Society at Harvard Kennedy School »), auxquelles ont participé environ 3000 personnes. La CNIL a assuré la coordination et la mise en cohérence de l'ensemble.

Les manifestations organisées dans le cadre du débat public ont aussi constitué l'occasion **de faire vivre dans la société française la réflexion sur des enjeux dont la prise de conscience par l'ensemble de nos contemporains, et pas seulement par les experts, est un enjeu civique et démocratique capital.**

Une concertation citoyenne : Montpellier, 14 octobre 2017

Les questions posées par les algorithmes et l'intelligence artificielle renvoient à des choix de société et concernent tous les citoyens. L'organisation d'une concertation a donc eu pour objectif de recueillir le point de vue de simples citoyens. Il s'agissait de compléter les réflexions émises à l'occasion de diverses manifestations ayant principalement donné la parole à des experts de différents secteurs.

Une journée de concertation a ainsi été organisée le 14 octobre 2017, avec le soutien de la Ville de Montpellier et de Montpellier Méditerranée Métropole. Un appel à candidature a permis de recruter un panel diversifié de 37 citoyens.

Le format retenu visait à **favoriser l'échange d'idées et la construction d'un avis collectif.** La technique d'animation a permis successivement aux participants de :

- Comprendre ce que sont les algorithmes et l'intelligence artificielle ;
- Analyser collectivement quatre études de cas (médecine et santé / ressources humaines / personnalisation et enfermement algorithmique / éducation et transparence) pour identifier les opportunités et les risques liés à l'usage des algorithmes ;
- Formuler des recommandations pour assurer le déploiement dans un cadre éthique des algorithmes et de l'IA, le degré de consensus de celles-ci ayant ensuite été évalué.

Les résultats et enseignements sont présentés dans les encadrés « Le regard du citoyen ».

La composition du rapport

Les manifestations organisées par les partenaires, ainsi que la concertation citoyenne, ont fait l'objet de restitutions recueillies par la CNIL. Les réflexions émises par des acteurs pluriels (syndicats, associations, entreprises, chercheurs, citoyens, etc.) dans des secteurs très divers (de l'assurance à l'éducation, en passant par la justice et la santé) ont ainsi alimenté le présent rapport, qui constitue un panorama général des questions éthiques soulevées par les algorithmes et l'intelligence artificielle dans leurs applications actuelles et dans leurs promesses à relativement court terme.

Animatrice du débat public, la CNIL en est aussi la restitutrice. À cet égard, elle a assumé la composition du rapport, ce qui implique inévitablement certains choix. La ligne de conduite adoptée a consisté à rendre loyalement et pleinement compte de la pluralité des points de vue exprimés. C'est aussi ce qui explique que les recommandations formulées à la fin du rapport entendent moins clore le débat que laisser ouvertes un certain nombre d'options possibles (dimension incitative ou obligatoire des mesures proposées, par exemple) qui devraient faire l'objet d'arbitrages ultérieurs. Il s'agit donc d'éclairer la décision publique et non de s'y substituer.

La CNIL s'est également appuyée pour la rédaction du rapport sur un travail de recherche documentaire, souvent initié sur la recommandation de tel ou tel partenaire. Les articles ou ouvrages utilisés ont été mentionnés en notes de bas de page. On pourra également se reporter aux pages du site de la CNIL consacrées au débat éthique pour retrouver quelques éléments de bibliographie sommaire[1]. Enfin, ont été exploités les résultats d'un certain nombre de travaux déjà conduits par diverses institutions en France et à l'étranger (entre autres, l'OPECST, la CERNA, le CNNUM, le Conseil d'Etat, la CGE, la Maison Blanche, France IA, INRIA, AI Now).

> Les questions posées par les algorithmes et l'intelligence artificielle renvoient à des choix de société et concernent tous les citoyens

1 https://www.cnil.fr/fr/ethique-et-numerique-les-algorithmes-en-debat-1

LES DATES CLÉS

7 OCTOBRE 2016

La CNIL obtient pour mission par la loi « République Numérique » de conduire une réflexion sur les enjeux éthiques et de société soulevés par les nouvelles technologies

23 JANVIER 2017

La CNIL annonce pour 2017 le thème des algorithmes et de l'intelligence artificielle et organise des tables-rondes de lancement réunissant des experts de ces sujets

FIN MARS 2017

Les premiers événements sont organisés par les partenaires du débat public

DÉBUT OCTOBRE 2017

45 événements se sont tenus, à l'initiative des **60 partenaires** du débat public

14 OCTOBRE 2017

La CNIL organise une concertation citoyenne à Montpellier réunissant près de **40 citoyens**

15 DÉCEMBRE 2017

La CNIL présente le rapport « **Comment permettre à l'Homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle** », synthèse du débat public

LES CHIFFRES CLÉS

45 ÉVÉNEMENTS

60 PARTENAIRES

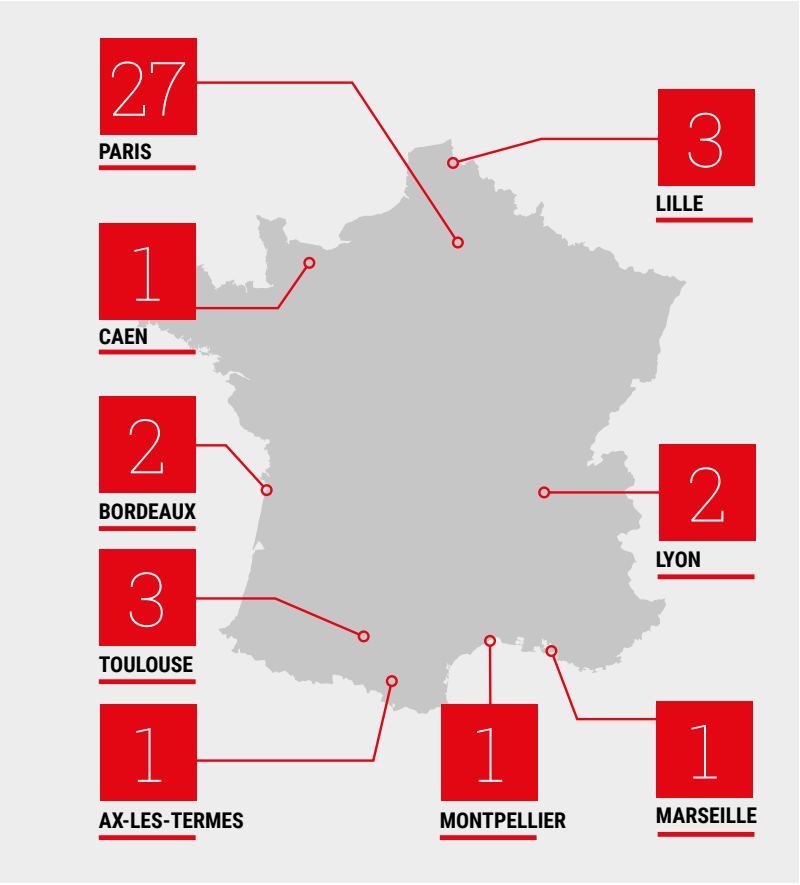
1 JOURNÉE DE CONCERTATION CITOYENNE

ENVIRON **3 000** PERSONNES PRÉSENTES LORS DES MANIFESTATIONS

27 À PARIS

14 EN PROVINCE

4 OUTRE ATLANTIQUE



Algorithmes et Intelligence artificielle aujourd'hui

Algorithmes et IA aujourd'hui

Un effort de définition nécessaire à la qualité du débat public

Algorithmes et intelligence artificielle sont à la mode. Ces mots sont aujourd'hui partout, non sans confusion parfois. Les définitions et les exemples qui en sont donnés dans le débat public aujourd'hui sont souvent imprécis. Ils sont parfois même contradictoires. Cette situation s'explique par le caractère très technique de sujets qui se sont trouvés rapidement mis en circulation et en débat dans un espace public dépassant largement les cercles d'experts et de spécialistes auxquels ils se sont longtemps trouvés cantonnés.

De là, pour peu que l'on y prête attention, une extrême imprécision dans les termes employés. **Quoi de commun entre l'austère notion d' « intelligence artificielle » définie dans les milieux de la cybernétique dans les années 1950 et sa représentation populaire diffusée notamment par le cinéma hollywoodien ?** Qui prête d'ailleurs attention au fait qu' « intelligence » n'a pas la même signification en français et en anglais, langue dans laquelle a été créé le vocable *« artificial intelligence »* ? Comment comprendre que l'on dise ici que les algorithmes sont nouveaux et que d'autres voix nous assurent que l'homme y a recours depuis plusieurs milliers d'années ?

Outre les réalités et les projets techniques qu'ils entendent désigner, les algorithmes et l'intelligence artificielle en sont venus à constituer de nouvelles mythologies de notre temps, dont la simple évocation suffit à connoter la modernité et l'innovation numériques. Rien d'étonnant dès lors à ce que ces termes soient apposés de manière souvent rapide et peu justifiée à des réalités ou à des entreprises soucieuses de se forger une image flatteuse et futuriste : présenter son activité comme relevant du domaine de l'IA est aujourd'hui pour de nombreux acteurs un enjeu d'image, comparable à celui représenté depuis quelques années par l'invocation d'un « Big data » dont les spécialistes soulignent pourtant souvent qu'il demeure une réalité aux dimensions encore modestes. En tout état de cause, la réalité des promesses de l'IA est aujourd'hui un sujet de controverses plus ou moins explicites entre chercheurs en intelligence artificielle, entrepreneurs et prescripteurs d'opinions divers dans le domaine des technologies.

Comme on le rappellera par la suite, un autre type de confusion semble parfois entretenu par des acteurs dont l'activité est généralement reconnue comme relevant du domaine de l'intelligence artificielle. Ces derniers majoreraient résolument et exagérément non tant les promesses que les risques d'une intelligence artificielle qui parviendrait à s'autonomiser totalement de son créateur au point de mettre en danger l'humanité. Les voix les plus compétentes s'élèvent pour battre en brèche de telles prévisions, assimilées au mieux à des fantasmes, voire à des mensonges. Ceux-ci auraient pour fonction de détourner l'attention publique des

> Fonder une discussion publique saine et constructive sur les sujets des algorithmes et de l'intelligence artificielle nécessite absolument de préciser le rapport entre algorithmes et intelligence artificielle

problèmes certes plus prosaïques mais plus pressants soulevés par le déploiement de l'intelligence artificielle, en matière de lutte contre les discriminations ou de protection des données personnelles par exemple.

Disons-le d'emblée : toute définition en ces matières pourra être sujette à caution selon les différents points de vue. Dans la perspective du présent rapport, l'essentiel est de parvenir à une base de discussion minimale et opératoire qui permette de tracer pragmatiquement le périmètre des algorithmes et de l'intelligence artificielle sources de questions éthiques et de société cruciales. Autrement dit, il s'agit de proposer une définition aussi rigoureuse que possible mais prenant en compte la perception commune de ce en quoi algorithmes et IA constituent aujourd'hui des enjeux dignes d'attention.

ENQUÊTE

Algorithmes et IA : un objet mal connu des Français*

Les algorithmes sont présents dans l'esprit des Français mais de façon assez confuse. Si **83% des Français ont déjà entendu parler des algorithmes,** ils sont **plus de la moitié à ne pas savoir précisément de quoi il s'agit** (52%). Leur présence est déjà appréhendée comme massive dans la vie de tous les jours par 80% des Français qui considèrent, à 65%, que cette dynamique va encore s'accentuer dans les années qui viennent.

83 %
des Français ont déjà entendu parler des algorithmes

* Sondage mené par l'IFOP pour la CNIL en janvier 2017 (auprès d'un échantillon de 1001 personnes, représentatif de la population française âgée de 18 ans et plus) sur le niveau de notoriété des algorithmes au sein de la population française.

Les algorithmes : une réalité ancienne au cœur de l'informatique

Au sens strict, un algorithme est la description d'une suite finie et non ambigüe d'étapes (ou d'instructions) permettant d'obtenir un résultat à partir d'éléments fournis en entrée. Par exemple, une recette de cuisine est un algorithme, permettant d'obtenir un plat à partir de ses ingrédients[2]. L'existence d'algorithmes utilisés pour résoudre des équations est d'ailleurs attestée très anciennement, dès le IIIe millénaire en Mésopotamie babylonienne.

Dans le monde de plus en plus numérique dans lequel nous vivons, **les algorithmes informatiques permettent de combiner des informations les plus diverses pour produire une grande variété de résultats : simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, piloter de façon autonome des automobiles ou des sondes spatiales, etc.**

Pour qu'un algorithme puisse être mis en œuvre par un ordinateur, il faut qu'il soit exprimé dans un langage informatique, transcrit en un programme (une sorte de texte composé de commandes écrites, également appelé « code source »). Ce programme peut alors être exécuté dans un logiciel ou compilé sous la forme d'une application. Un logiciel a recours en général à de nombreux algorithmes : pour la saisie des données, le calcul du résultat, leur affichage, la communication avec d'autres logiciels, etc.

2 Voir par exemple : http://www.cnrtl.fr/definition/algorithme

Des algorithmes à l'intelligence artificielle

Peu de notions font aujourd'hui l'objet d'un usage plus mouvant que celle d' « intelligence artificielle » (IA). Le choix a été fait dans ce rapport de se concentrer pragmatiquement sur les usages d'ores et déjà effectifs de l'intelligence artificielle et, plus précisément, sur ceux qui ont fait l'objet des plus rapides développement au cours des dernières années, en lien avec les progrès du *machine learning* (ou apprentissage automatique).

De façon large, l'intelligence artificielle peut être définie comme « la science qui consiste à faire faire aux machines ce que l'homme ferait moyennant une certaine intelligence » (Marvin Minsky). Si c'est en 1956, lors de la conférence de Darmouth que naît formellement la notion d'intelligence artificielle dans le milieu de la cybernétique, on peut considérer comme point de départ l'article publié en 1950 par Alan Turing *(Computing Machinery and Intelligence)* où celui-ci pose la question de savoir si les machines peuvent penser. Les chercheurs de cette discipline naissante ambitionnent de doter des ordinateurs d'une intelligence généraliste comparable à celle de l'homme, et non pas limitée à certains domaines ou à certaines tâches.

L'histoire de l'intelligence artificielle depuis les années 1950 n'a pas été celle d'un progrès continu. En premier lieu, les chercheurs se sont vus contraints de délaisser l'objectif visant à mettre au point une IA généraliste (ou « IA forte ») pour se concentrer sur des tâches plus spécifiques, sur la résolution de problèmes tels que la reconnaissance d'images, la compréhension du langage naturel ou la pratique de jeux (jeu de dames, échecs, jeu de go, par exemple). On parle dès lors d' « IA faible », car spécialisée. Même si l'on s'en tient au domaine de l'IA faible, l'histoire de ce champ de recherche et de ses applications est marquée par des discontinuités. À une période d'optimisme dans les années 1980 a succédé à partir des années 1990 un « hiver de l'IA » : les progrès se sont heurtés à une insuffisance tant de la puissance de calcul que des données disponibles, notamment.

Ces dernières années ont au contraire été marquées par une série de succès spectaculaires qui ont remis au goût du jour les promesses de l'IA. La victoire d'Alpha Go (Google) contre le champion du monde de jeu de Go, Lee Sedol, en mars 2016, a constitué symboliquement le plus notable de ces événements. Contrairement au jeu d'échecs, le go, du fait de la multiplicité innombrable des combinaisons qu'il permet, ne se prête pas à la mémorisation d'un grand nombre de parties que la machine pourrait se contenter de reproduire.

La victoire d'Alpha Go illustre le fait que les développements récents de l'IA sont notamment liés au perfectionnement de la technique du *machine learning* (apprentissage automatique), qui en constitue l'une des branches. Alors que le programmeur doit traditionnellement décomposer en de multiples instructions la tâche qu'il s'agit d'automatiser de façon à en expliciter toutes les étapes, l'apprentissage automatique consiste à alimenter la machine avec des exemples de la tâche que l'on se propose de lui faire accomplir. L'homme *entraîne* ainsi le système en lui fournissant des données à partir desquelles celui-ci va *apprendre* et déterminer lui-même les opérations à effectuer pour accomplir la tâche en question. Cette technique permet de réaliser des tâches hautement plus complexes qu'un algorithme classique. Andrew Ng, de l'Université Stanford, définit ainsi le *machine learning* comme « la science permettant de faire agir les ordinateurs sans qu'ils aient à être explicitement programmés ». Cela recouvre la conception, l'analyse, le développement et la mise en œuvre de méthodes permettant à une machine d'évoluer par un processus systématique, et de remplir des tâches difficiles. L'intelligence artificielle qui repose sur le *machine learning* concerne donc des algorithmes dont la particularité est d'être conçus de sorte que leur comportement évolue dans le temps, en fonction des données qui leur sont fournies.

L'apprentissage profond *(Deep learning)* est le socle des avancées récentes de l'apprentissage automatique, dont il est l'une des branches[3]. **On distingue apprentissage automatique supervisé[4]** (des données d'entrées qualifiées par des humains sont fournies à l'algorithme qui définit donc des règles à partir d'exemples qui sont autant de cas validés) **et non supervisé[5]** (les données sont fournies brutes à l'algorithme qui élabore sa propre classification et est libre d'évoluer vers n'importe quel état final lorsqu'un motif ou un élément lui est présenté). L'apprentissage supervisé nécessite que des instructeurs apprennent à la machine les résultats qu'elle doit fournir, qu'ils l'« entraînent ». Les personnes entraînant l'algorithme remplissent en fait souvent une multitude de tâches très simples. Des plateformes telles que le « Mechanical Turk » d'Amazon sont les lieux où se recrutent ces milliers de « micro-tâcherons » (Antonio Casilli) qui, par exemple, étiquettent les immenses

3 Il s'agit d'un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires. Sa logique étant inspirée du fonctionnement des neurones, on parle souvent de « réseaux neuronaux ».

4 Un algorithme de *scoring* de crédit utilisera cette technique : on fournit l'ensemble des caractéristiques connues des clients et de leur emprunt en indiquant ceux qui n'ont pas remboursé leur crédit, et l'algorithme sera capable de fournir un score de risque de non remboursement pour les futurs clients.

5 Un algorithme de détection des typologies de fraudes utilisera cette technique : on fournit à l'algorithme toutes les données relatives à des fraudes avérées, et l'algorithme sera capable de dégager des similitudes entre ces fraudes, et de dégager des typologies de fraudes. L'apprentissage non supervisé peut aussi servir à identifier, sur la bande sonore d'une émission de radio, les séquences de parole de différents locuteurs.

FOCUS

L'exemple de la reconnaissance d'images

La reconnaissance d'images permet de prendre la mesure de ce qui distingue algorithmes classiques et algorithmes de *machine learning* (que le vocabulaire courant confond aujourd'hui généralement avec l'IA). Imaginons que l'on ait pour objectif de faire reconnaître les tigres à une machine. Si l'on se proposait d'y parvenir au moyen d'un algorithme classique, il faudrait imaginer pouvoir décrire explicitement en langage de programmation la totalité des opérations intellectuelles que nous réalisons lorsque nous identifions que nous avons à faire à un tigre et non pas, par exemple, à tout autre animal, voire à un lion ou à un chat. Si distinguer un tigre d'un chat ne pose aucun problème même à un jeune enfant, en décomposer et expliciter l'ensemble des étapes nécessaires à reconnaitre un tigre (autrement dit, en donner l'*algorithme*) s'avère être une tâche, sinon impossible du moins d'une ampleur rédhibitoire. C'est ici qu'intervient la technique du machine learning. Il s'agit de fournir à la machine des exemples en grande quantité, en l'occurrence de très nombreuses photographies de tigres, ainsi que des photographies d'autres animaux. À partir de ce jeu de données, la machine apprend à reconnaître des tigres. Elle élabore elle-même, par la confrontation des milliers de photographies qui lui sont fournies, les critères sur lesquels elle s'appuiera pour reconnaître des tigres dans des photographies qui lui seront ultérieurement soumises.

Il s'agit ici d' « apprentissage supervisé » : c'est bien l'homme qui fournit à la machine des milliers de photographies qu'il a préalablement identifiées comme représentant des tigres ainsi que d'autres explicitement identifiées comme ne représentant *pas* des tigres.

quantités de photographies utilisées pour entraîner un logiciel de reconnaissance d'images. Le système de captcha de Google « recaptcha » est un autre exemple d'utilisation à grande échelle d'humains pour entrainer des machines. Ces algorithmes d'apprentissage sont utilisés dans un nombre croissant de domaines, allant de la prédiction du trafic routier à l'analyse d'images médicales.

On comprend à travers l'exemple de la reconnaissance d'images (voir encadré) en quoi l'intelligence artificielle ouvre la voie à l'automatisation de tâches incomparablement plus complexes que l'algorithmique classique. L'IA, contrairement aux algorithmes déterministes construit elle-même à partir des données qui lui sont fournies les modèles qu'elle va appliquer pour appréhender les réalités qui lui sont soumises. Ainsi s'explique qu'elle s'avère aujourd'hui particulièrement prometteuse dans des secteurs produisant des quantités énormes de données, telles que la météorologie.

Les exemples d'utilisation de l'intelligence artificielle sont d'ores et déjà nombreux, bien au-delà du seul domaine de la reconnaissance de formes. Ainsi, la classification du spam parmi les messages reçus sur Gmail constitue une application caractéristique, dans sa simplicité même, de l'IA.

LE SAVIEZ-VOUS ?

Une entreprise comme Airbus mobilise aujourd'hui concrètement l'intelligence artificielle à des fins de reconnaissance de forme. Apprendre à un système à reconnaître sur une photographie aérienne d'une zone maritime les différents navires présents peut servir, par exemple, à confronter l'emplacement des embarcations ainsi repérées aux signaux émis par les balises et à identifier des navires en perdition ou qui cherchent à se soustraire à la surveillance maritime. L'intérêt réside dans la rapidité d'une opération qui, si elle n'est pas automatisée, réclame un temps et des moyens considérables. Depuis quelques années, les progrès de ces techniques sont tels que la machine surpasse désormais l'humain pour la fiabilité de l'identification de navires parfois difficilement distinguables de nuages.

Le signalement par les usagers de messages considérés comme indésirables permet à Google de constituer une base conséquente et constamment alimentée à partir de laquelle le système peut apprendre à déterminer les caractéristiques des spams qui vont ensuite lui permettre de proposer de lui-même quels messages filtrer. Toujours chez Google, l'intelligence artificielle est à l'œuvre dans le service de traduction automatique. L'entreprise explique également avoir eu recours au *machine learning* pour analyser le fonctionnement du système de refroidissement de ses *data centers*. L'automatisation de cette fonction d'analyse aurait ainsi permis de réduire de 40 % l'énergie nécessaire au refroidissement de ces installations.

L'utilisation industrielle de l'IA n'est pas nouvelle : elle s'est notamment développée dans les années 1980, quand les « systèmes experts » ont permis d'optimiser l'opération de vidange des cuves des centrales nucléaires, automatisant les calculs et renforçant du même coup leur fiabilité en permettant de substantielles économies liées à la réduction de la durée d'immobilisation des installations à des fins de maintenance.

Les robots conversationnels (chat bots) et assistants vocaux (comme Siri, Google Assistant ou Alexa) constituent un autre pan en rapide développement de l'intelligence artificielle : ils peuvent par exemple fournir des informations et répondre à des questions standardisées.

À la lumière de ces applications, on comprend donc en quoi **le *machine learning* constitue à strictement parler une rupture par rapport à l'algorithmique classique.** Avec les algorithmes apprenants, c'est bien une nouvelle classe d'algorithmes qui émerge : on passe progressivement « d'un monde de programmation à un monde d'apprentissage » (Jean-Philippe Desbiolles, événement de lancement du débat public, CNIL, 23 janvier 2017). Les algorithmes classiques sont déterministes, leurs critères de fonctionnement sont explicitement définis par ceux qui les mettent en œuvre. Les algorithmes apprenants, au contraire, sont dits probabilistes. S'ils constituent une technologie bien plus puissante que les algorithmes classiques, leurs résultats sont mouvants et dépendent à chaque instant de la base d'apprentissage qui leur a été fournie et qui évolue elle-même au fur et à mesure de leur utilisation. Pour reprendre l'exemple du tigre (voir encadré), il est possible qu'une intelligence artificielle ayant été entraînée sur une base dans laquelle figure une seule espèce de tigres ne soit pas à même de reconnaître un tigre appartenant à une autre espèce. Mais on peut supposer qu'elle puisse aussi élargir sa capacité à reconnaître d'autres espèces de tigres à force d'être confrontée à de plus en plus d'individus partageant des traits communs aux deux races.

Au-delà de ces différences techniques, une approche globale des algorithmes et de l'IA demeure cependant pertinente. Algorithmes déterministes et algorithmes apprenants soulèvent en effet des problèmes communs. Dans un cas comme dans l'autre, la finalité des applications de ces classes d'algorithmes consiste à automatiser des tâches autrement accomplies par des humains, voire à déléguer à ces systèmes automatisés des prises de décisions plus ou moins complexes. Dès lors que l'on se détache d'une appréhension strictement technique de ces objets pour en aborder les conséquences et les implications sociales, éthiques, voire politiques, les problèmes posés se recoupent largement et méritent de faire l'objet d'une investigation conjointe.

Précisons enfin qu'algorithmes et intelligence artificielle recoupent à bien des égards ce que l'on appelle, de façon généralement imprécise, « Big data ». Le Big data désigne non seulement d'immenses quantités de données diverses mais également les techniques qui permettent de les traiter, de les faire parler, d'y repérer des corrélations inattendues, voire de leur conférer une capacité prédictive. De même, l'intelligence artificielle est indissociable des immenses quantités de données nécessaires pour l'entraîner et qu'elle permet en retour de traiter.

> L'algorithme sans données est aveugle. Les données sans algorithmes sont muettes

Cadrer la réflexion en fonction des applications et des impacts les plus cruciaux des algorithmes aujourd'hui

En un sens l'algorithmique recouvre l'informatique et croise plus généralement tout ce qu'on a coutume d'englober sous le terme de « numérique ».

Face à un sujet potentiellement aussi vaste, il est donc aussi nécessaire que légitime de limiter le périmètre de la réflexion aux algorithmes qui posent aujourd'hui les questions éthiques et de société les plus pressantes. **La réflexion éthique sur les systèmes d'IA et sur les algorithmes n'a en effet de sens que si elle prend aussi en compte l'inscription de ceux-ci dans des contextes sociaux, humains, professionnels.**

Les pages qui suivent envisageront ainsi les usages de l'intelligence artificielle en limitant cette dernière aux usages s'appuyant sur le *machine learning,* qui sont les plus discutés aujourd'hui même si, en toute rigueur, ils ne constituent pas l'entièreté de ce domaine[6].

Par ailleurs, il a été décidé d'exclure du champ de la réflexion les problèmes soulevés par l'IA forte (ou générale). L'IA forte désigne des systèmes susceptibles de devenir complètement autonomes qui pourraient même se retourner contre l'homme. Cette vision se nourrit souvent d'un imaginaire apocalyptique alimenté par le cinéma hollywoodien dans le sillage de mythes parfois bien plus anciens (Frankenstein, etc.). Elle est souvent reliée à une interrogation concernant le niveau de conscience de soi d'une telle machine (en lien avec le thème de la singularité technologique). Elle est par ailleurs propagée par des prises de positions de personnalités du numérique disposant d'une forte visibilité médiatique, comme Elon Musk ou Stephen Hawking. Enfin, la diffusion du thème de la « singularité » par les milieux transhumanistes rayonnant depuis la Silicon Valley renforce les discours annonçant le dépassement prochain de l'homme par les machines. Force est pourtant de constater qu'elle est accueillie avec scepticisme par les plus éminents chercheurs et experts en informatique, comme en France Jean-Gabriel Ganascia. **L'hypothèse de l'avènement d'une IA forte est même dénoncée par certains (dont ce dernier) comme un moyen d'éluder de plus sérieux problèmes – éthiques voire tout simplement juridiques – que posent déjà et à brève échéance les progrès effectifs de l'IA faible et son déploiement croissant.**

Il aurait été possible, en toute rigueur et en prenant les termes au pied de la lettre, d'inclure dans le périmètre de notre réflexion sur les algorithmes les questions liées au chiffrement dans la mesure où cette technologie repose sur l'utilisation d'algorithmes. Le même procédé aurait pu conduire à considérer la « blockchain » comme partie intégrante du sujet. Là encore, il a semblé préférable d'adopter une attitude pragmatique, guidée par la perception publique de ce que sont aujourd'hui les algorithmes et leurs applications soulevant le plus de problèmes et d'interrogations. En d'autres termes, nous avons choisi de limiter le champ de la réflexion à ceux des algorithmes qui, dans l'immense diversité qui est la leur à l'ère numérique, soulèvent aujourd'hui des problèmes susceptibles d'interpeller directement le grand public et les décideurs, tant publics que privés.

À cet égard, les **algorithmes de recommandation,** s'ils ne constituent techniquement qu'une fraction des différents types d'algorithmes, constituent une partie importante de la question. Les algorithmes de recommandation sont employés pour établir des modèles prédictifs à partir d'une quantité importante de données et les appliquer en temps réel à des cas concrets. Ils élaborent des prévisions sur des comportements ou des préférences permettant de devancer les besoins des consommateurs, d'orienter une personne vers le choix jugé le plus approprié pour elle... Ces algorithmes peuvent par exemple être utilisés pour proposer des restaurants sur un moteur de recherche.

Si l'on prolonge cette approche, on peut lister ainsi les **principales fonctions et applications des algorithmes** susceptibles de faire débat et sur lesquelles la présente réflexion est centrée :

6 Les deux grandes approches de l'IA sont, d'une part, l'approche symboliste et cognitiviste et, d'autre part, l'approche neuro-inspirée et connexionniste (apprentissage automatique, réseaux de neurones, etc.). Les systèmes experts ont connu un important développement dans les années 1980. Les principales avancées récentes reposent sur l'apprentissage automatique.

- Produire des connaissances ;
- Apparier une demande et une offre (« matching »), répartir des ressources (passagers et chauffeurs de taxis, parents et places en crèche, étudiants et places à l'université, etc.) ;
- Recommander un produit, une offre de façon personnalisée ;
- Aider la prise de décision ;
- Prédire, anticiper (par exemple, des phénomènes naturels, des infractions, la survenue d'une maladie).

Ces grandes fonctions découlent de la capacité des algorithmes à filtrer l'information, à modéliser des phénomènes en identifiant des motifs parmi de grandes masses de données et à profiler les individus[7].

D'une manière générale, **la visibilité accrue des algorithmes et des questions qu'ils posent aujourd'hui est indissociable des masses de données inédites à disposition dans tous les secteurs qu'il faut trier pour pouvoir en tirer tout le potentiel.** La numérisation de notre société sous toutes ses formes – dématérialisation des transactions et services, révolution des capteurs, de l'Internet des objets, diffusion du smartphone, généralisation des politiques d'*open data,* etc. – est à l'origine de cette profusion. Celle-ci constitue aujourd'hui une ressource mais aussi un défi : **si nous avons besoin de recommandations, c'est que l'offre informationnelle est devenue pléthorique ; s'il est possible de profiler, c'est que la quantité de données collectées sur les individus permet de dépasser la segmentation par catégories prédéterminées.** L'enjeu soulevé par la qualité et la pertinence des données disponibles ou choisies pour alimenter les algorithmes constitue un autre point essentiel que rencontre toute réflexion à l'égard de ceux-ci.

Il faut aussi introduire l'idée d'**autonomisation,** pour bien prendre la mesure des enjeux soulevés par les algorithmes aujourd'hui. Si les algorithmes posent question, c'est aussi parce qu'ils permettent de déléguer des tâches auparavant accomplies par l'homme à des systèmes automatiques de plus en plus « autonomes ». Cependant, la délégation de tâches voire de décisions à des algorithmes traditionnels n'implique nullement que la production des algorithmes elle-même échappe à l'homme. L'intervention humaine est bien présente dans le recours aux algorithmes, par l'intermédiaire du paramétrage de l'algorithme, du choix et de la pondération des critères et des catégories de données à prendre en compte pour arriver au résultat recherché. Par exemple, si l'humain n'intervient pas directement dans la recommandation d'un restaurant par le biais d'une plateforme algorithmique, en revanche le rôle des développeurs est fondamental. En effet, ces derniers déterminent notamment l'importance que pourra jouer la localisation des restaurants, leur notation par d'autres usagers ou encore sa concordance supposée (là encore en fonction de critères à définir) avec le profil du requêteur.

Avec le développement du machine learning, on se situe un pas plus loin dans cette dynamique d'autonomisation, la machine écrivant « elle-même » les instructions qu'elle exécute, déterminant les paramètres qui doivent la guider dans le but d'accomplir une finalité qui reste cependant définie par l'homme.

> La visibilité accrue des algorithmes aujourd'hui est indissociable des masses de données inédites à disposition dans tous les secteurs, qu'il faut trier pour pouvoir en tirer tout le potentiel

7 Le profilage est défini par le Règlement européen sur la protection des données à caractère personnel comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

Des usages et des promesses dans tous les secteurs

Les usages des algorithmes et de l'intelligence artificielle se développent dans tous les secteurs. Un discours porté très énergiquement par les acteurs économiques met en avant les avantages et les promesses de ces outils. On en mentionnera ici quelques exemples tout en renvoyant pour plus de détails aux **fiches sectorielles présentes en annexe et traçant les contours des grandes applications des algorithmes** que les débats ont permis d'évoquer[8].

Les usages aujourd'hui les plus banalisés ont trait, notamment, aux moteurs de recherche sur internet, aux applications de navigation routière, à la recommandation sur les plateformes de contenu culturel (type Netflix ou Amazon) ou sur les réseaux sociaux, au marketing pour le ciblage publicitaire et, de plus en plus, pour la prospection électorale.

Dans le domaine de la santé publique, l'utilisation des algorithmes est mise en avant pour la veille sanitaire (détection d'épidémies, de risques psycho-sociaux). On évoque de plus en plus les promesses d'une médecine de précision bâtissant des solutions thérapeutiques personnalisées en croisant les données du patient à celles de gigantesques cohortes.

Les fonctions régaliennes de l'État sont également concernées par l'émergence d'acteurs prétendant, par exemple, fournir des outils d'aide aux professions juridiques qui permettraient, à partir du traitement de données de jurisprudence, d'anticiper l'issue d'un procès ou d'affiner une stratégie judiciaire. Les services de police, en France et à l'étranger, commencent quant à eux à recourir à des outils algorithmiques destinés, par l'analyse de données, à orienter leurs efforts vers tel ou tel secteur.

Le débat largement médiatisé autour d' « APB » a mis en lumière aux yeux du grand public le recours à l'algorithme pour la répartition de centaines de milliers d'étudiants dans les universités. Au-delà de la gestion des flux, l'algorithme interroge les pratiques pédagogiques par des stratégies de personnalisation de l'enseignement toujours plus fines ou par la détection possible de décrochages scolaires.

ENQUÊTE

Une connaissance inégale des usages des algorithmes*

L'intervention d'algorithmes est bien repérée par le public lorsqu'il s'agit d'un usage tel que le ciblage publicitaire (90 % des sondés en ont conscience).

Elle est en revanche souvent moins clairement perçue en ce qui concerne l'évaluation de la « compatibilité amoureuse » sur des applications de rencontre (46 % des répondants) ou l'élaboration d'un diagnostic médical (33 %).

* Enquête réalisée dans le cadre du débat public par l'association « Familles rurales », association familiale orientée vers les milieux ruraux, auprès de 1076 de ses adhérents.

Sur le marché de l'emploi, enfin, de nombreux acteurs travaillent actuellement au développement de solutions d'aide au recrutement (par appariement de l'offre et de la demande d'emploi, notamment) et de gestion des ressources humaines.

Sans prétendre épuiser un objet aux applications innombrables, le tableau qui figure à la page suivante donne cependant une idée de la façon dont les grandes fonctions identifiées des algorithmes et de l'intelligence artificielle se retrouvent dans différents secteurs.

8 Le développement industriel de l'intelligence artificielle est porté principalement par deux types d'acteurs. D'une part, des spécialistes de la fourniture de technologies et de services aux grandes entreprises, comme IBM avec Watson. D'autre part, les grands industriels de la donnée numérique (dont les GAFA), qui investissent fortement et chargent leurs services en IA (comme Google avec Translate, la reconnaissance d'images ou le traitement automatique de la parole).

Les grandes fonctions des algorithmes et de l'IA dans différents secteurs

	Education	Justice	Santé	Sécurité	Travail, RH	Culture	Autres
Générer de la connaissance	Mieux cerner les aptitudes d'apprentissage des élèves	Mettre en évidence les manières différenciées de rendre la justice selon les régions	Tirer profit de la quantité immense de publications scientifiques	Repérer des liens insoupçonnés pour la résolution d'enquêtes par les services de gendarmerie	Comprendre les phénomènes sociaux en entreprise	Créer des œuvres culturelles (peinture, musique)	Affiner le profil de risque d'un client d'un assureur
Faire du matching	Répartir les candidats au sein des formations d'enseignement supérieur (APB)		Répartir des patients pour participation à un essai clinique		Faire correspondre une liste de candidatures avec une offre d'emploi		Mettre en relation des profils « compatibles » sur des applications de rencontres, etc.
Prédire	Prédire des décrochages scolaires	Prédire la chance de succès d'un procès et le montant potentiel de dommages-intérêts	Prédire des épidémies Repérer des prédispositions à certaines pathologies afin d'en éviter le développement	Détecter les profils à risque dans la lutte anti-terroriste Prédire l'occurrence future de crimes et délits	Détecter les collaborateurs qui risquent de démissionner dans les prochains mois	Créer des œuvres ayant un maximum de chance de plaire aux spectateurs (Netflix)	
Recommander	Recommander des voies d'orientation personnalisées aux élèves	Recommander des solutions de médiation en fonction du profil des personnes et des cas similaires passés			Proposer des orientations de carrière adaptées aux profils des personnes	Recommander des livres (Amazon), des séries télévisées (Netflix), etc.	Individualiser des messages politiques sur les réseaux sociaux
Aider la décision		Suggérer au juge la solution jurisprudentielle la plus adéquate pour un cas donné	Suggérer au médecin des solutions thérapeutiques adaptées	Suggérer aux forces de police les zones prioritaires dans lesquelles patrouiller			Aider le conducteur à trouver le chemin le plus court d'un point à un autre (GPS)

Les enjeux éthiques

Les enjeux éthiques

L'éthique, éclaireuse du droit

La notion d'éthique fait souvent l'objet d'usages différents, laissant parfois place à une forme d'ambigüité. Les définitions proposées par les dictionnaires renvoient l'éthique à la morale, autrement dit à des normes qui n'ont pas nécessairement vocation à entrer dans le droit et qui portent sur la conduite des individus. Chez les philosophes antiques, l'éthique n'est ainsi rien d'autre que la réponse à la question suivante : « qu'est-ce qu'une vie bonne ? », c'est-à-dire des principes d'action qui concernent d'abord l'individu.

Plus récemment, la notion d'éthique s'est notamment développée comme renvoyant à une forme d'à côté du droit, évoqué entre autres par des acteurs privés comme les entreprises. L'éthique est alors un ensemble de normes édictées par l'entreprise et qu'elle s'impose à elle-même. Ces normes peuvent aller au-delà du droit. Souvent, elles peuvent n'avoir pour principale fonction que de redire – consciemment ou pas – des normes juridiques. Certaines évocations de l'utilisation « éthique » des données du client ne sont parfois rien d'autre qu'une façon de dire que l'entreprise se plie à la loi.

Un troisième usage de la notion d'éthique – sans doute le plus pertinent dans le contexte du présent rapport – s'est développé dans le langage des institutions publiques depuis la création en 1983 du Comité Consultatif National d'Ethique pour les sciences de la vie et de la santé (CCNE). Dans ce cadre, **l'éthique apparaît comme une éclaireuse du droit, la norme éthique une préfiguration de la norme juridique.** Que le législateur demande à une institution de produire une réflexion éthique place bien à l'horizon – plus ou moins proche – d'une telle réflexion l'inscription législative de celle-ci. La création par la loi du CCNE partageait un point commun important avec celle de la Loi pour une République numérique et sa création d'une mission de réflexion éthique confiée à la CNIL : un contexte marqué par de rapides avancées technologiques et par de fortes incertitudes sur l'attitude que la collectivité avait à adopter face à celles-ci. D'une part, les progrès de la biotechnologie (le premier bébé-éprouvette français naît en 1982), de l'autre

ENQUÊTE

Une perception publique des algorithmes et de l'IA empreinte de méfiance*

Les trois craintes les plus partagées sont la **perte de contrôle humain** (63 % des adhérents), la **normativité** et l'enfermement à travers l'uniformisation des recrutements (56 %) et la **collecte disproportionnée de données personnelles** (50 %).

Dans le champ de l'emploi, quelques opportunités sont mises en exergue comme la possibilité d'examiner toutes les candidatures sur la base de critères identiques (52 %). Toutefois, **72 % des répondants envisagent comme une menace la possibilité d'être recruté par des algorithmes,** sur la base d'une analyse de leur profil et de sa compatibilité à un poste défini. 71 % d'entre eux affirment ainsi que la définition d'une charte éthique autour de l'usage des algorithmes constitue une réelle priorité.

72 %
des répondants envisagent comme une menace la possibilité d'être recruté par des algorithmes

* Enquête réalisée dans le cadre du débat public par la CFE-CGC, syndicat de l'encadrement, auprès de 1263 de ses adhérents (essentiellement issus des fédérations « Métallurgie » et « Finance et Banque »).

ce qui est ressenti comme une « révolution numérique ». L'inscription dans la loi d'une réflexion éthique répond donc au besoin d'un espace nécessaire pour une réflexion collective sur un pacte social dont certains aspects essentiels (libertés fondamentales, égalité entre les citoyens, dignité humaine) peuvent être remis en question dès lors que l'évolution technologique déplace la limite entre le possible et l'impossible et nécessite de redéfinir la limite entre le souhaitable et le non souhaitable.

La CNIL a choisi pour cette première réflexion de s'appuyer sur les acteurs désireux de s'exprimer sur les sujets liés aux algorithmes et à l'intelligence artificielle. Les enjeux éthiques retenus sont donc ceux qui ont été évoqués par ces mêmes acteurs. De manière logique, ces enjeux sont pour la plupart déjà bel et bien présents dans nos sociétés, même s'ils sont probablement appelés à gagner en intensité dans les années à venir. En revanche, des enjeux plus prospectifs, liés à des progrès pour l'heure hypothétiques des technologies numériques (transhumanisme, hybridation homme-machine, etc.), ont peu mobilisé la réflexion des partenaires impliqués et sont de ce fait peu développés dans le rapport.

> L'évolution technologique déplace la limite entre le *possible* et l'*impossible* et nécessite de redéfinir la limite entre le *souhaitable* et le *non souhaitable*

LE REGARD DU CITOYEN

Les participants à la concertation citoyenne organisée par la CNIL à Montpellier le 14 octobre 2017 se sont prononcés sur les questions éthiques posées par les algorithmes et l'intelligence artificielle (voir « Une démarche innovante au service de l'élaboration d'une réflexion éthique collective et pluraliste ») : les enjeux qu'ils soulèvent résonnent en grande partie avec ceux identifiés tout au long du débat public.

Les citoyens semblent prioritairement préoccupés par les nouvelles modalités de prise de décision et la dilution de la responsabilité créées par l'algorithme. La « **perte de compétence** » **éventuelle de médecins ou d'employeurs** qui se reposeraient intensément sur l'algorithme a été mise en exergue. Parmi les conséquences préjudiciables évoquées : une « gestion des incertitudes » jugée inefficace chez la machine comparativement à ce dont est capable l'homme ; une incapacité à « gérer les exceptions » ou encore la « perte du sentiment d'humanité » (évoquées notamment à propos de l'absence de recours sur « APB »).

Le recours à des systèmes informatiques, parfois autonomes, pour prendre des décisions fait craindre que la **responsabilité** en cas d'erreurs ne soit « pas claire », une préoccupation soulevée notamment à propos du secteur médical. Concernant le cas « APB », certains citoyens critiquent le manque de transparence qui explique que l'algorithme serve « de bouc émissaire faisant tampon entre ceux qui font des choix politiques et ceux qui se plaignent de ces choix ». La problématique de la personnalisation informationnelle sur les réseaux sociaux et de ses effets collectifs, évoquée au sujet des élections présidentielles aux Etats-Unis, accentue également leur crainte que « plus personne ne soit réellement responsable du contrôle d'Internet ».

Moins évoqué, le danger de l'enfermement algorithmique est cependant mentionné par plusieurs participants des ateliers « ressources humaines » et « plateformes numériques ». Les citoyens ont aussi évoqué le risque de « **formatage** » des recrutements, et la rationalisation consécutive d'un champ qui ne devrait pas autant l'être, ou encore celui d'être figé sur Internet « dans un profil qui freinerait nos évolutions personnelles ».

Enfin, la thématique **des biais, des discriminations et de l'exclusion** mérite une vigilance toute particulière aux yeux des participants, et cela que les biais en question soit volontaires (en matière de recrutement, on craint l'éventualité qu'un algorithme soit codé « selon les objectifs des employeurs aux dépens des salariés ») ou involontaires (l'outil algorithmique est facteur d'inquiétudes quant aux erreurs qu'il pourrait générer).

L'autonomie humaine au défi de l'autonomie des machines

Au-delà de la multiplicité des applications pratiques et des utilisations qui peuvent en être faites, **algorithmes et intelligence artificielle ont pour objet commun d'accomplir automatiquement une tâche ou une opération impliquant une forme d'« intelligence » qui serait autrement effectuée directement par un agent humain.** Autrement dit, il s'agit pour l'homme de **déléguer des tâches à des systèmes automatiques**[9].

Le cas d'APB en offre un bon exemple. Ce logiciel détermine l'affectation des bacheliers dans l'enseignement supérieur. Il peut être considéré comme ne faisant rien d'autre que d'appliquer un ensemble d'instructions et de critères qui pourraient tout aussi bien l'être par des fonctionnaires. L'intérêt essentiel du recours à l'algorithme est dans ce cas le gain de productivité induit par la délégation d'une tâche très coûteuse en temps et en moyens à un système automatique. Un autre intérêt de l'algorithme est de garantir le déploiement uniforme et impartial des règles définies en amont pour la répartition des futurs étudiants. En effet, l'application de ces mêmes règles par une chaîne administrative complexe peut donner prise, bien plus facilement, à des formes d'arbitraires ou même tout simplement à des interprétations différentes selon les agents qui les appliquent. Spécialiste des politiques éducatives, Roger-François Gauthier n'hésite ainsi pas à affirmer qu'APB a au moins eu le mérite de mettre fin à un système « mafieux » où le passe-droit avait sa place[10].

Si APB est un algorithme déterministe classique, l'utilisation de la **reconnaissance de formes pour identifier en temps réel des embarcations sur les photographies satellitaires** de très vastes surfaces maritimes fournit quant à elle une illustration de la façon dont l'intelligence artificielle permet aussi d'accomplir des tâches qui pourraient autrement s'avérer trop coûteuses en ressources humaines. Un simple logiciel peut ainsi assurer la surveillance 24 heures sur 24 de zones immenses qui nécessiterait autrement l'activité de nombreuses personnes.

De façon plus prospective, il serait au moins techniquement envisageable de confier – comme cela se fait déjà aux Etats-Unis – à des algorithmes le soin d'évaluer la dangerosité d'un détenu et donc l'opportunité d'une remise de peine. L'étape supplémentaire de ce que certains appellent la « justice prédictive » serait de confier à des systèmes le soin d'établir des décisions sur la base de l'analyse des données du cas à juger croisées aux données de jurisprudence.

La délégation de tâches aux algorithmes : des situations contrastées

Il semble d'emblée assez évident que **les implications éthiques et sociales potentielles du phénomène accru de délégation de tâches à des systèmes automatisés présentent des degrés assez variés de sensibilité** selon les tâches qu'il s'agit de déléguer et selon les modalités mêmes de cette délégation.

Il est ainsi possible de faire un pas supplémentaire pour distinguer les cas sur lesquels la réflexion doit se concentrer, au moyen d'**une typologie du phénomène de délégation d'opérations à des systèmes automatisés,** en fonction de deux critères : **l'impact sur l'homme de l'opération qu'il s'agit de déléguer et le type de système à qui il est question de déléguer celle-ci.**

Le premier critère concerne le type d'impact et/ou l'ampleur de l'opération déléguée au système automatisé. Il peut s'agir d'une tâche routinière, mécanique et relativement anodine (par exemple, le classement par ordre alphabétique d'une série de fichiers informatiques). À l'opposé, cette tâche peut perdre son caractère anodin et s'avérer d'une grande complexité. Elle peut, surtout, prendre les aspects d'une *décision* et revêtir une importance vitale pour une personne ou pour un groupe, comme lorsqu'il s'agit d'établir une aide au diagnostic médical. Entre ces deux extrêmes se déploie un large spectre de situations contrastées. On y retrouverait les deux exemples évoqués ci-dessus ou encore celui de la voiture autonome, ce dernier ainsi que le cas d'APB étant relativement plus proches du cas du diagnostic médical automatisé que de l'autre bout du spectre.

Le second critère concernerait quant à lui le type de système automatisé – algorithme classique ou algorithme de *machine learning* – à qui l'on délègue l'opération. Une autre façon de présenter ce critère est d'évoquer le **degré d'autonomie du système** en question, en particulier sa capacité ou non à élaborer ses propres critères de fonctionnement. De même, ce critère renvoie à la capacité ou non du système de produire une explication satisfaisante des résultats qu'il fournit.

Cette typologie souligne la grande diversité des situations impliquées par une réflexion sur les enjeux éthiques et sociaux des algorithmes et de l'intelligence artificielle. Elle met surtout en évidence l'étendue du spectre sur lequel peut

9 En toute rigueur, rappelons-le, ce n'est d'ailleurs généralement pas tant le recours à l'algorithme qui constitue le fait nouveau que son exécution sous la forme d'un programme informatique.
10 Événement de lancement du débat public, CNIL, 23 janvier 2017.

se situer le degré de gravité ou de sensibilité des enjeux liés à l'utilisation de tel ou tel algorithme.

La délégation de décisions critiques aux algorithmes: une déresponsabilisation ?

Les décisions les plus cruciales (diagnostics médicaux, décisions judiciaires, décision d'ouvrir le feu dans un contexte de conflit armé etc.) qui pourraient être, voire commencent à être (à l'étranger notamment) déléguées à des systèmes automatisés sont – au moins dans certains cas – déjà clairement thématisées par la tradition juridique, en France. Seul un médecin est ainsi habilité à établir un diagnostic qui, autrement, relèverait de l'exercice illégal de la médecine. Il en va de même de la décision du juge, qui ne saurait en toute rigueur être déléguée à un système automatisé. Dans cette perspective, ce type de système est présenté dans ces domaines comme une « aide » à la prise de décision.

Cette clarté juridique ne résout cependant pas les problèmes que soulève l'éventualité d'une délégation de ce type de décisions. Comment s'assurer que la prédiction et la recommandation fournies par les algorithmes ne soient effectivement qu'une aide à la prise de décision et à l'action humaine sans aboutir à une déresponsabilisation de l'homme, à une perte d'autonomie ?

Dans le domaine médical où la qualité de la prise de décision peut être plus facilement évaluée (ou, du moins, quantifiée), on peut logiquement se demander quelle marge d'autonomie resterait au médecin face à la recommandation (en termes de diagnostic et de solution thérapeutique à privilégier) qui serait fournie par un système d'« aide » à la décision extrêmement performant. On annonce en effet que l'intelligence artificielle serait supérieure à l'homme pour le diagnostic de certains cancers ou pour l'analyse de radiographies. Dans le cas où ces annonces s'avéreraient exactes, il pourrait donc devenir hasardeux pour un médecin d'établir un diagnostic ou de faire un choix thérapeutique autre que celui recommandé par la machine, laquelle deviendrait dès lors le décideur effectif. Dans ce cas, se pose alors la question de la responsabilité. Celle-ci doit-elle être reportée sur la machine elle-même, qu'il s'agirait alors de doter d'une personnalité juridique ? Sur ses concepteurs ? Doit-elle être encore assumée par le médecin ? Mais alors, si cela peut certes sembler résoudre le problème juridique, cela n'aboutit-il quand même pas à une déresponsabilisation de fait, au développement d'un sentiment d'irresponsabilité ?

FOCUS

Les défis éthiques d'une police prédictive

La quête d'une prédiction du crime dans le temps et dans l'espace serait capable de prédire le crime dans le temps et dans l'espace, afin d'orienter l'action des patrouilles, fait l'objet d'un développement actif de logiciels algorithmiques. Aux Etats-Unis, « **PredPol** » s'appuie sur des modèles empruntés à la sismologie pour évaluer l'intensité du risque à tel endroit et à tel moment. La start-up prétend ainsi intégrer la dimension « contagieuse » de la diffusion spatiotemporelle des délits.

Ce potentiel prédictif s'est pourtant révélé limité, d'une part, car la contagion a un impact négligeable pour la détection de crimes comparativement aux répliques d'un séisme et, d'autre part, car la structure de la criminalité varie d'une année à l'autre. Pourtant, cela ne dissipe pas l'attrait de tels dispositifs consistant à permettre de ***« gérer, selon des critères gestionnaires, l'offre publique de vigilance quotidienne ».*** Très concrètement, *« le carré prédictif reste rouge sur la carte tant que la police n'y a pas patrouillé, il tourne ensuite au bleu lors des premiers passages, puis il apparaît en vert lorsque le policier a passé le temps suffisant et optimal calculé selon les ressources disponibles »*[11].

Une crainte majeure émerge : quid du risque que les préconisations de la machine soient appréhendées comme une vérité absolue, non soumise à la discussion quant à ses conséquences pratiques ? Dans la mesure où l'algorithme se repose sur les données issues des plaintes des victimes, une conséquence pratique constatée est celle d'une présence policière renforcée dans les zones où les publics portent plainte avec plus de fluidité, et ainsi un phénomène d'exclusion de l'offre de sécurité publique pour certaines populations (celles qui signalent moins). On peut imaginer, au contraire, que l'utilisation de ce type d'algorithme focalise l'attention policière sur certains types d'infractions au détriment d'autres.

Dans tous les cas, une appréhension critique de ce type d'outil est une nécessité majeure. Quid également de la capacité à juger de l'efficacité de ces modèles ? Qu'un délit soit détecté par une patrouille orientée par le système, ou que ce ne soit pas le cas, le résultat pourrait facilement (mais faussement) être interprété comme un signe de l'efficacité de l'outil.

11 Bilel Benbouzid, « A qui profite le crime ? Le marché de la prédiction du crime aux Etats-Unis », www.laviedesidees.fr

Le cas de la médecine est particulièrement critique non seulement en raison de l'impact des décisions et recommandations sur les personnes mais aussi en raison du fait que la discussion implique ici des systèmes fondés sur la technologie du *machine learning*. Ceci implique que les logiques sous-jacentes des systèmes d'intelligence artificielle sont potentiellement incompréhensibles pour celui à qui ils sont proposés, autant d'ailleurs que pour les concepteurs du système. Le débat public organisé par la CNIL a d'ailleurs été l'occasion de constater une controverse sur ce point, à propos notamment du logiciel Watson d'IBM. Le discours d'IBM souligne que Watson fonctionne sur le mode de l' « apprentissage supervisé ». Autrement dit, le système est accompagné pas à pas dans son apprentissage, ce qui permettrait d'en contrôler la logique, par opposition à un apprentissage non supervisé qui reviendrait effectivement à laisser une pleine et entière autonomie à la machine pour déterminer ses critères de fonctionnement. IBM indique également contrôler le fonctionnement des systèmes avant de décider de conserver l'apprentissage réalisé. Au contraire, les chercheurs experts de ce domaine qui ont eu l'occasion de s'exprimer lors des différents débats organisés (et notamment la CERNA) ont régulièrement rappelé qu'en l'état actuel de la recherche les résultats fournis par les algorithmes de machine learning les plus récents n'étaient pas explicables. Cette explicabilité constitue d'ailleurs l'objet de recherches en cours. Ils insistent également sur le fait qu'il est très difficile de contrôler effectivement un système de *machine learning*.

On peut ainsi se demander si les algorithmes et l'intelligence artificielle ne conduisent pas à une forme de dilution de figures d'autorité traditionnelles, de décideurs, de responsables, voire de l'autorité même de la règle de droit. Cette évolution est parfois explicitement souhaitée. Certains, comme Tim O'Reilly, imaginent d'ores et déjà l'avènement d'une « réglementation algorithmique[12]» qui verrait la « gouvernance » de la cité confiée aux algorithmes : grâce aux capteurs connectés, lieux, infrastructures et citoyens communiqueraient en permanence des données traitées en vue de rationaliser et d'optimiser la vie collective selon des lois considérées comme « naturelles », émanant des choses mêmes, une « normativité immanente », comme l'expliquent Thomas Berns et Antoinette Rouvroy[13]. Sans doute faut-il remarquer ici que la tentation – révélée par ces discours – de se passer d'une normativité humaine et de préférer une normativité algorithmique est favorisée par les discours marchands. Ces derniers vantent l' « objectivité » supposée des systèmes automatiques (par opposition à un jugement humain toujours faillible). Ils influent donc sur la tendance des utilisateurs à prendre le résultat produit par une machine pour une vérité incontestable, alors même qu'il est de part en part déterminé par des choix (de critères, de types de données fournies au système) humains[14].

L'impact des algorithmes sur la conception et l'application de la norme pourrait aussi prendre une autre forme. Le Conseil National des Barreaux, dans le rapport qu'il a remis à la CNIL, souligne ainsi qu'**« il faut éviter que l'obsession de l'efficacité et de la prévisibilité qui motive le recours à l'algorithme nous conduise à concevoir les catégories et les règles juridiques non plus en considération de notre idéal de justice mais de manière à ce qu'elles soient plus facilement « codables » ».**

Il n'est pas exclu que cette évolution progressive vers des formes de « réglementation algorithmique » puisse présenter une sorte d'attrait pour les décideurs eux-mêmes. Déléguer des décisions à une machine – supposée neutre, impartiale, infaillible – peut être une façon d'éluder sa propre responsabilité, de s'exempter de la nécessité de rendre compte de ses choix. Le **développement d'armes létales autonomes (robots tueurs)** qui pourraient prendre elles-mêmes la décision de tuer sur le champ de bataille ou à des fins de maintien de l'ordre soulève la question avec une particulière acuité. L'acte de tuer, même considéré comme légitime, dans une situation de conflit international et face à un ennemi armé, ne doit-il pas rester sous le contrôle et la responsabilité directe de l'homme ? Sa difficulté et son caractère éventuellement traumatique pour celui-là même qui l'accomplit ne doivent-ils pas être considérés comme une garantie nécessaire pour éviter toute dérive ?

Ces considérations ne concernent pas que les situations où des tâches ou des décisions sont déléguées à un algorithme apprenant. L'algorithme classique, déterministe, est également concerné. Les débats autour de l'algorithme d'APB en ont offert un bon exemple, sinon une manière de comprendre comment **peut se mettre en place un tel processus de dépolitisation et de neutralisation de choix de société méritant pourtant de faire l'objet d'une discussion publique.** La polémique s'est en effet concentrée sur l'algorithme lui-même, notamment à la suite de la révélation de la mise en œuvre du tirage au sort qu'il induisait pour certains candidats à des filières en tension. Or, l'algorithme n'est jamais que le reflet de choix politiques, de choix de société. En l'occurrence, le recours au tirage au sort pour l'attribution de places dans des filières en tension est le résultat d'un choix politique dont deux alternatives possibles seraient – schématiquement – la sélection à l'entrée à l'université ou l'investissement pour faire correspondre le nombre de places disponibles dans les filières en question avec la demande. En d'autres termes, « code is law », pour reprendre la fameuse formule de Lawrence Lessig.

12 Tim O'Reilly, « Open data and algorithmic regulation », in Brett Goldstein (dir.), Beyond Transparency: Open Data and the Future of Civic Innovation, San Francisco, Code for America, 2013, pp. 289-301.
13 Rouvroy Antoinette, Berns Thomas, « Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? », Réseaux, 2013/1 (n° 177), p. 163-196.
14 La prétendue objectivité machinique n'est à ce titre qu'une subjectivité diluée et non assumée.

On ne saurait en effet considérer qu'un algorithme (entendu au sens large comme le système socio-technique dont il fait partie) puisse être « neutre », dans la mesure où il incorpore inévitablement des partis pris – que ceux-ci soient sociaux, politiques, éthiques ou moraux – et répond le plus souvent à des finalités qui incluent une dimension commerciale pour son auteur. L'exemple fréquemment évoqué du choix que pourrait être amené à faire l'algorithme d'une voiture sans chauffeur de sacrifier ou bien son occupant ou bien un piéton sur la route illustre la façon dont le recours à la technique, plus que de soulever certains problèmes moraux, a surtout pour effet de les déplacer : à un dilemme réglé en temps réel par une personne impliquée dans sa chair fait place un choix effectué par d'autres, ailleurs, bien en amont[15].

Au-delà de la finalité délibérément visée à travers la mise en place d'APB (efficacité administrative renforcée et harmonisation plus équitable de l'attribution de places dans l'enseignement supérieur), force est de constater que celle-ci a pour effet induit l'escamotage de choix de société impliqués par le paramétrage du système mais masqués par l'impartialité supposée de l'algorithme. Les responsables de la mise en œuvre de l'algorithme auquel est déléguée une prise de décision devraient donc chercher des moyens de contrer ce type d'effets (par exemple, par un effort d'information du public concerné). Ils devraient en tout cas s'interdire de l'exploiter en se cachant derrière la machine ou même de s'en accommoder dans la mesure où il a tendance à neutraliser des conflits ou des débats légitimes.

> Les algorithmes et l'intelligence artificielle conduisent à une forme de dilution de figures d'autorité traditionnelles, de décideurs, de responsables, voire de l'autorité même de la règle de droit

Il est d'ailleurs probable que céder à cette facilité ait pour contrepartie un sentiment d'inhumanité chez les personnes concernées. Ce sentiment est susceptible de se transformer en rejet, en particulier si n'est prévue aucune possibilité de contacter l'organisme responsable et d'échanger pour « trouver des solutions ou tout simplement pour être écouté », ainsi que l'a souligné le médiateur de l'Éducation nationale[16].

Dans le cas d'un algorithme déterministe tel qu'évoqué ici, la dilution de la responsabilité n'est pourtant qu'apparente. Les choix et les décisions cruciales se trouvent tout simplement déplacés au stade du paramétrage de l'algorithme.

Est-ce à dire que ceux qui maîtrisent le code informatique deviennent les véritables décideurs et que se profile le risque que le pouvoir se trouve concentré dans les mains d'une « petite caste de scribes » (Antoine Garapon, événement de lancement du débat, le 23 janvier 2017) ? Ce n'est certes pas ce qu'a donné à voir le cas d'APB. Suite à l'ouverture du code source des algorithmes de l'administration qu'a imposée la loi pour une République numérique, celui d'APB a été examiné par la mission Etalab. Il s'est avéré que ses développeurs avaient pris soin d'y documenter l'origine de chaque modification du paramétrage de l'algorithme, en l'occurrence les directives qu'ils avaient reçues de la part de l'administration. En somme, la traçabilité de la responsabilité a été organisée par les développeurs mêmes d'APB. Cet exemple ne doit cependant pas masquer le fait que la logique algorithmique a tendance à déporter la prise de décision vers les étapes techniques de conception d'un système (paramétrage, développement, codage), lequel ne fait ensuite que déployer automatiquement et sans faille les choix opérés initialement. La préoccupation d'Antoine Garapon évoquée précédemment ne saurait donc pas être écartée et appelle des réponses. **Il est essentiel que ces étapes de conception ne s'autonomisent pas exagérément au point de devenir le lieu de la prise de décision.**

La question du lieu de la responsabilité et de la décision se pose en partie différemment dès lors qu'il s'agit de systèmes de *machine learning*. Sans doute faut-il ici davantage penser en termes de chaîne de responsabilité, depuis le concepteur du système jusqu'à son utilisateur, en passant par celui qui va entraîner ce système apprenant. En fonction des données qui lui auront été fournies, ce dernier se comportera différemment, en effet. On peut penser ici au cas du robot conversationnel Tay mis en place par Microsoft et suspendu au bout de 24 heures quand, alimenté par des données d'utilisateurs des réseaux sociaux, il avait commencé à tenir des propos racistes et sexistes. Reste qu'organiser précisément la répartition de la responsabilité entre

15 Voir à ce sujet l'excellent site du MIT offrant une illustration pratique de ces dilemmes : http://moralmachine.mit.edu/
16 Le Monde, 29 juin 2016 : « Le médiateur de l'Education Nationale dénonce la solitude des familles face à APB ».

ces différents maillons de la chaîne est un problème ardu. Au-delà, **faut-il conditionner l'utilisation de l'intelligence artificielle à la capacité d'attribuer de façon absolument claire cette responsabilité ?** On sait d'ores et déjà que des intelligences artificielles peuvent être plus « performantes » que l'homme pour réaliser certaines tâches, sans que l'on ait une claire compréhension du fonctionnement de ces systèmes et donc, aussi, des erreurs éventuelles qu'ils pourraient commettre. Rand Hindi explique ainsi que « les IA font moins d'erreurs que les humains mais qu'elles font des erreurs là où des humains n'en auraient pas fait. C'est ce qui est arrivé avec l'accident de la voiture autonome de Tesla, qui ne serait jamais arrivé avec un humain ». Faut-il alors imaginer d'attribuer une personnalité juridique à ces systèmes ? Ou faire endosser la responsabilité à l'utilisateur lui-même (en l'occurrence, dans le domaine médical, au patient) ?

Sans doute ne faut-il toutefois pas exagérer la spécificité du cas du *machine learning*. Imaginons une intelligence artificielle chargée de répartir les malades dans les services d'un hôpital et de fixer la fin de leur hospitalisation de la manière la plus « efficace » possible. Certainement, le système aurait une part d'opacité liée à son caractère apprenant. Mais, dans le même temps, les objectifs qui lui seraient assignés, ainsi que leur pondération (garantir le maximum de guérisons à long terme, minimiser le taux de réhospitalisations à brève échéance, rechercher la brièveté des séjours, etc.), seraient bien des choix explicitement faits par l'homme.

Une question d'échelle : la délégation massive de décisions non critiques

La réflexion éthique sur les algorithmes et l'intelligence artificielle doit-elle se cantonner à considérer les décisions cruciales, les secteurs où l'impact sur l'homme est incontestable, comme la médecine, la justice, l'orientation scolaire, voire l'automobile, avec ses implications en termes de sécurité ? **Ne faut-il pas prendre en compte également les algorithmes à qui nous sommes amenés à déléguer progressivement de plus en plus de tâches et de décisions apparemment anodines mais qui, mises bout à bout, constituent l'étoffe de nos existences quotidiennes ?**

Simplement par leur capacité à fonctionner de façon répétée, sur de longues durées et surtout à de très vastes échelles, les algorithmes peuvent avoir un impact considérable sur les personnes ou sur les sociétés. Par exemple, les critères de fonctionnement d'une banale application de guidage automobile, dès lors qu'ils sont utilisés par un nombre conséquent d'automobilistes qui s'en remettent implicitement à eux pour décider des itinéraires qu'ils empruntent, peuvent avoir des impacts importants sur le trafic urbain, la répartition de la pollution et à terme, peut-être, sur la forme même de la ville et de la vie urbaine. Le Laboratoire d'innovation numérique (LINC) de la CNIL l'explique ainsi : « Hormis la question de la captation des données personnelles, se pose celle de la perte de contrôle de l'acteur public sur l'aménagement de l'espace public, sur la gestion des flux, et au-delà sur la notion même de service public et d'intérêt général. La somme des intérêts individuels des clients d'un Waze peut parfois entrer en contradiction avec les politiques publiques portées par une collectivité[17] ».

Cathy O'Neil, dans son ouvrage *Weapons of Math Destruction*[18], propose un exemple particulièrement évocateur. Elle imagine qu'elle pourrait modéliser les règles qu'elle suit implicitement pour composer les repas de ses enfants (diversité, présence de légumes verts mais dans des limites permettant de prévenir de trop fortes protestations, relâchement des règles les dimanches et jours de fête, etc.). Un programme mettant en œuvre un tel algorithme ne poserait pas de problème tant qu'il ne serait utilisé pour générer automatiquement des repas que pour un nombre limité de personnes. Or, la caractéristique spécifique des algorithmes exécutés par des programmes informatiques est leur échelle d'application. Un tel programme, utilisé tel quel par des millions de personnes, aurait nécessairement des impacts puissants et potentiellement déstabilisateurs sur de grands équilibres sociaux et économiques (renchérissement du prix de certaines denrées, effondrement de la production d'autres produits, uniformisation de la production, impact sur les professions de la filière agro-industrielle, etc.). **C'est ici un aspect bien spécifique des algorithmes informatiques déployés aujourd'hui à l'heure d'Internet qui constitue le fait nouveau et que l'auteur met en évidence : leur *échelle* de déploiement.** Sans doute cet aspect ne saurait-il être ignoré par ceux qui déploient des algorithmes susceptibles d'être utilisés à une large échelle.

L'optimisation algorithmique comme écrasement du temps et de l'espace

L'une des caractéristiques du fonctionnement algorithmique est son immédiateté et sa simplicité, du moins son uniformité et son caractère inexorable. Les algorithmes d'IA ont la capacité d'accomplir une tâche dans un temps presque immédiat (réduit au temps du seul calcul de la machine). Ils ont la capacité d'accomplir cette même tâche à une très large échelle spatiale mais de façon identique en tous lieux. À ce titre, ils peuvent présenter un grand attrait pour des administrations ou des entreprises soucieuses d'efficacité mais aussi de rationalité et d'homogénéité de leur action.

17 CNIL (LINC), La Plateforme d'une ville. Les données personnelles au cœur de la fabrique de la smart city, Cahier IP n°5, octobre 2017, p. 20.
18 Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown, 2016.

Or, cette caractéristique des algorithmes implique aussi une dimension potentiellement problématique : **l'écrasement de la durée et de la dimension spatiale du processus délégué à la machine peut aussi constituer une perte, un appauvrissement de l'action.** Les cas des algorithmes utilisés par l'administration ainsi que celui de la justice prédictive permettent de mieux saisir cette ambivalence, entre optimisation et appauvrissement de processus vidés de leur dimension spatiale.

Ainsi, le déploiement d'un algorithme comme celui du logiciel APB peut certes être considéré comme garant pour l'administration d'une forme de simplicité et d'harmonisation de l'application des règles, là où le fonctionnement d'une chaîne administrative complexe et nombreuse peut donner prise à des différences d'interprétation et d'application. Pourtant, ce qui peut apparaître à première vue comme un manque d'efficacité ou comme le signe d'un fonctionnement parfois erratique ne peut-il pas être aussi considéré comme une source précieuse d'information pour les décideurs, via les retours d'expériences et les questionnements de ceux qui sont chargés d'appliquer les règles et peuvent en observer le déploiement et éventuellement les limites, au plus près du terrain ?

De même, le colloque sur la justice prédictive organisé le 19 mai 2017 par le Barreau de Lille, la Faculté de droit de l'Université catholique de Lille et la cour d'appel de Douai a vu certains participants souligner que « la connaissance des décisions rendues par les autres juridictions voisines ou par les autres magistrats contribuera à une certaine harmonie et évitera que l'issue d'un litige dépende de la question de savoir s'il est plaidé à Lille ou à Marseille ». L'idée repose ici sur la capacité des algorithmes à traiter les grandes masses de données de jurisprudence mises en open data et à mettre en évidence des disparités d'application de la loi dans différentes juridictions. Le dévoilement de ces disparités dont le juge n'a pas lui-même conscience aurait pour conséquence une harmonisation de l'application de la loi sur le territoire national. Pourtant, est-on absolument certain que, dans certaines limites, des formes de disparités régionales ne traduisent pas en fait un usage raisonné de la prudence du juge et l'adaptation intelligente et fine de celui-ci à des réalités sociales pouvant varier d'un lieu à l'autre ? Une forme de respiration de la loi, peut-être, à distinguer de son application automatique et rigide ?

On peut appliquer le même type de raisonnement à l'idée d'une justice prédictive qui, poussée à son extrême (une décision de justice rendue par une intelligence artificielle), éluderait l'apport de la délibération en commun et de ce qui peut s'y jouer à travers la confrontation d'individualités partageant un objectif commun. **La délibération de jurés et de magistrats n'est pas que le simple déploiement d'arguments préexistants à la manière dont un logiciel « exécute » un programme. La durée n'y est pas qu'un décor accessoire, une ressource dont il conviendrait de limiter la dépense : elle y est un acteur à part entière.** Elle implique la capacité des jurés à évoluer au cours de l'échange d'arguments, à changer de positions, ainsi que le montre mieux que toute démonstration le film de Sidney Lumet, *Douze hommes en colère*.

Il semble en tout cas souhaitable d'attirer l'attention des utilisateurs d'algorithmes et d'intelligence artificielle sur la nécessité de ne pas prendre en compte seulement les apports, mais aussi les inconvénients éventuels de ces technologies, leur caractère potentiellement ambivalent, et de réfléchir aux moyens de les contrer.

Biais, discriminations et exclusion

La propension des algorithmes et de l'intelligence artificielle à générer des biais pouvant conduire à leur tour à créer ou à renforcer des discriminations s'est imposée comme un sujet d'inquiétude et de questionnement. Le constat mérite d'autant plus d'être souligné que ces systèmes techniques peuvent également parfois nourrir une croyance en leur objectivité. Une objectivité d'autant plus précieuse qu'elle ferait souvent défaut aux humains. Tout algorithme est pourtant, en un sens, biaisé, dans la mesure où il est toujours le reflet – à travers son paramétrage et ses critères de fonctionnement, ou à travers les données d'apprentissage qui lui ont été fournies – d'un système de valeurs et de choix de société. Le débat autour des biais et des discriminations qu'ils peuvent générer n'est donc qu'un miroir grossissant mettant en valeur cette caractéristique essentielle dans ce qu'elle a de plus problématique.

Plusieurs exemples ont récemment illustré de façon particulièrement nette et choquante ce type de biais. En 2015, un logiciel de reconnaissance faciale de Google a ainsi suscité une forte polémique. Un jeune couple d'Afro-Américains s'est rendu compte qu'une de ses photos avait été

étiquetée sous le tag « gorille ». L'explication de ce dysfonctionnement réside dans le type de données avec lesquelles l'algorithme a été entraîné pour reconnaître des personnes. En l'occurrence, il est vraisemblable qu'il l'ait été au moyen essentiellement, voire exclusivement, de photographies de personnes blanches (d'autres exemples existent d'ailleurs de biais racistes de logiciels de reconnaissance d'image au détriment de personnes de type « asiatique »). En conséquence, l'algorithme a considéré qu'une personne de couleur noire présentait plus de similitude avec l'objet « gorille » qu'elle avait été entrainée à reconnaitre qu'avec l'objet « humain ».

Notons d'ailleurs que des actes de malveillance volontaires de la part de personnes impliquées dans le processus d'entraînement de ce type d'algorithmes ne sont pas exclus. Ainsi en a-t-il été pour le robot conversationnel Tay développé par Microsoft et qui s'est mis à proférer sur Twitter des propos racistes et sexistes après quelques heures de fonctionnement et d'entraînement au contact des propos que lui adressaient des internautes.

Les biais des algorithmes peuvent aussi être des biais de genre. En 2015, trois chercheurs de l'Université Carnegie Mellon et de l'International Computer Science Institute ont mis en évidence la façon dont Adsense, la plateforme publicitaire de Google, générait un biais au détriment des femmes. À l'aide d'un logiciel baptisé Adfisher, ils ont créé 17 000 profils dont ils ont ensuite simulé la navigation sur le Web afin de mener une série d'expériences. Ils ont ainsi constaté que **les femmes se voyaient proposer des offres d'emploi moins bien rémunérées que celles adressées à des hommes, à niveau similaire de qualification et d'expérience.** Il est apparu qu'un nombre restreint de femmes recevaient des annonces publicitaires en ligne leur proposant un emploi au revenu supérieur à 200 000 dollars annuels. Loin d'être anecdotique, « la publicité en ligne ciblée de Google est tellement omniprésente que l'information proposée aux personnes est susceptible d'avoir un effet tangible sur les décisions qu'elles prennent », souligne Anupam Datta, co-auteur de l'étude.

Ici encore, les causes précises sont difficiles à établir. Il est bien sûr envisageable qu'un tel biais soit le fruit d'une volonté des annonceurs eux-mêmes : ceux-ci auraient alors délibérément choisi d'adresser des offres différentes aux hommes et aux femmes. Mais il est tout aussi possible que ce phénomène soit aussi le résultat d'une réaction de l'algorithme aux données qu'il a reçues. En l'occurrence, les hommes auraient pu avoir davantage tendance en moyenne à cliquer sur les publicités annonçant les emplois les mieux rémunérés tandis que les femmes auraient eu tendance à s'autocensurer, selon des mécanismes bien connus des sciences sociales. Dès lors, le biais sexiste de l'algorithme ne serait pas autre chose que la reproduction d'un biais préexistant dans la société.

FOCUS

Des algorithmes contre la récidive ?

Les applications de justice prédictive font l'objet d'une attention publique toute particulière quant à leurs potentiels effets discriminatoires. Une polémique a éclaté autour de l'application COMPAS (Correctional Offender Management Profile for Alternative Sanction) visant à produire un **score de risque de récidive** pour les détenus ou accusés lors d'un procès. Bien que des outils d'analyse statistique de données aient déjà été déployés au sein des tribunaux américains depuis les années 1970, un tel calcul automatique sous la forme de score revêt un caractère nouveau pour la prise de décisions de libération conditionnelle.

En d'autres termes, le travailleur social utilisant COMPAS a recours à une interface lui permettant de répondre, en collaboration avec le prévenu, à des questions du type « Que pense le prévenu de la police ? », « Quelles sont les caractéristiques des amis du prévenu ? », « Certains d'entre eux ont-ils déjà été condamnés ? »[19]. Un score de risque est ainsi calculé et ajouté au dossier du prévenu.

Le site ProPublica a accusé Nortphointe, société commercialisant COMPAS, de produire des scores **biaisés et racistes**[20]**.** Ce constat repose sur la confrontation des scores de récidive de détenus libérés avec l'observation, ou non, d'une arrestation sur une période de deux ans. Le taux de faux positifs (c'est-à-dire un score élevé mais sans récidive effective observée) s'est révélé considérablement plus fort pour les anciens détenus d'origine afro-américaine que pour les individus blancs.

19 https://usbeketrica.com/article/un-algorithme-peut-il-predire-le-risque-de-recidive-des-detenus
20 https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Troisième exemple, en avril 2016, il a été révélé qu'Amazon avait exclu d'un de ses nouveaux services (la livraison gratuite en un jour) des quartiers peuplés majoritairement de populations défavorisées à Boston, Atlanta, Chicago, Dallas, New York et Washington. À l'origine, un algorithme d'Amazon avait mis en évidence, en analysant les données à sa disposition, que les quartiers en question n'offraient guère de possibilités de profit pour l'entreprise. Même si l'objectif d'Amazon n'était assurément pas d'exclure de ses services des zones parce que leur population était majoritairement noire, tel s'avérait pourtant bien être le résultat de l'utilisation de cet algorithme : dans six grandes villes, il apparaît clairement que « l'aire de fourniture du service exclut les codes postaux à population majoritairement noire, à des degrés variés ». En conséquence, les citoyens noirs ont environ deux fois moins de chances que les blancs de vivre dans des zones desservies par [le service d'Amazon en question][21] ». À Boston, alors que la ville entière avait accès au service, seuls trois codes postaux en étaient exclus, dans le quartier majoritairement noir de Roxbury.

Comment expliquer ce phénomène, alors qu'Amazon a souligné – à juste titre, sans aucun doute – n'avoir recouru à aucune donnée raciale pour alimenter l'algorithme ? Il a été opposé à Amazon que les quartiers concernés étaient précisément les mêmes que ceux qui avaient fait l'objet pendant des décennies de la pratique dite du « redlining », consistant pour les banques à refuser systématiquement d'accorder des prêts à des Afro-Américains, même solvables, en raison de la couleur de leur peau et de leur domiciliation dans des zones peuplées majoritairement par des minorités. Il est donc évident que l'algorithme d'Amazon a pour effet de reproduire des discriminations préexistantes, quand bien même aucun racisme intentionnel n'est ici à l'œuvre.

Le paramétrage des algorithmes, c'est-à-dire la définition explicite des critères selon lesquels ils fonctionnent et opèrent des tris, sélectionnent et recommandent, peut bien sûr être la source de biais et de discrimination. Mais, comme le montrent les trois exemples évoqués ci-dessus, ce sont bien les biais provoqués par les données fournies aux systèmes qui soulèvent le défi le plus redoutable aujourd'hui. Le caractère historique d'un jeu de données confère à celui-ci la capacité à reproduire des inégalités ou des discriminations préexistantes. Un algorithme qui chercherait à définir les profils à recruter sur la base des profils ayant correspondu aux trajectoires de carrière les plus réussies dans le passé d'une entreprise pourrait ainsi tout à fait exclure les femmes, soit que celles-ci aient fait l'objet d'une exclusion dans le passé, soit qu'elles aient eu tendance à interrompre leurs carrières davantage que leurs collègues masculins, par exemple. On notera d'ailleurs que, pour l'entreprise en question, l'utilisation irraisonnée d'un tel algorithme aurait pour conséquence de se priver de talents. Le problème éthique croiserait ici directement l'enjeu d'efficacité.

> Inconscients chez ceux-là mêmes qui sélectionnent les données, les biais ne sont pas forcément sensibles pour les utilisateurs qui y sont sujets

Dès lors, l'opération même d'entraînement des algorithmes – à travers la sélection qu'elle suppose des données à prendre en compte – apparaît comme le cœur d'un enjeu éthique et juridique, et non pas seulement technique ou d'efficacité. Cet enjeu recoupe en partie celui de la délégation de prises de décisions, abordé précédemment : choisir quelles données sont utilisées pour les phases d'apprentissage revient bien à prendre des décisions parfois lourdes de conséquences. En revanche, le caractère spécifique de l'enjeu abordé ici tient au fait qu'il **s'agit de décisions et de choix qui peuvent être effectués de manière presque inconsciente** (alors que le codage d'un algorithme classique

LE SAVIEZ-VOUS ?

À l'occasion du débat organisé le 24 juin 2017 par le Génotoul (Toulouse), Philippe Besse, Professeur de mathématiques et de statistique à l'Université de Toulouse a souligné que nous ne sommes pas tous égaux devant la médecine personnalisée, car les bases de données utilisées à l'heure actuelle sont largement biaisées : une étude a révélée qu'en 2009, 96 % des échantillons de ces bases ont des ancêtres européens (la démonstration porte sur 1,5 million d'échantillons). D'autres sources de biais sont l'âge (car toutes ces bases de données sont largement occupées par des personnes relativement âgées) et le genre, plusieurs publications récentes insistant sur l'importance de l'effet du genre sur le développement des maladies concernées. Dans ces bases, le chromosome X est largement sous représenté et le Y est quasiment absent. Philippe Besse conclut ainsi : « si vous êtes une femme d'origine africaine et jeune, je ne pense pas que la médecine personnalisée vous concerne ».

21 https://www.bloomberg.com/graphics/2016-amazon-same-day/

et déterministe est toujours une opération délibérée). Celui qui entraîne un algorithme y insère d'une certaine façon sa propre vision du monde, ses valeurs ou, à tout le moins, des valeurs présentes plus ou moins directement dans les données tirées du passé. La chercheuse Kate Crawford, notamment, a ainsi mis en évidence l'endogamie sociale, raciale et de genre qui caractérise les milieux où se recrutent ceux qui entraînent aujourd'hui l'intelligence artificielle[22].

Tout ceci explique largement l'une des caractéristiques les plus problématiques de ces biais et des discriminations auxquelles ceux-ci peuvent donner lieu : ils sont souvent particulièrement difficiles à découvrir. Inconscients chez ceux-là mêmes qui sélectionnent les données, ils ne sont pas forcément sensibles pour les utilisateurs qui y sont sujets. Le caractère ciblé des offres d'emploi évoquées précédemment fait que les femmes concernées n'avaient pas connaissance des offres d'emploi proposées aux hommes. C'est l'une des conséquences du phénomène d'« enfermement algorithmique », dont il sera question plus loin. Enfin, les systèmes d'intelligence artificielle font quant à eux des choix dont la logique (voire l'existence même) échappe à leurs concepteurs.

En somme, les biais et les discriminations générées par les algorithmes soulèvent aujourd'hui deux questions majeures. Faut-il d'abord considérer au moins dans certains cas que l'intelligence artificielle ne fait jamais que reconduire des biais et des discriminations déjà existants dans la société ? En d'autres termes, les algorithmes ne seraient jamais ici que des « conducteurs » de biais, ils ne feraient que les répéter sans les créer eux-mêmes. On pourrait à tout le moins objecter à une telle position que l'échelle à laquelle ils se déploient et leur impact potentiel en font les lieux privilégiés pour la lutte contre les discriminations, que leur puissance, en somme, implique des obligations renforcées. Sans compter qu'il n'est pas exclu qu'ils puissent aussi avoir un effet démultiplicateur de ces biais.

Deuxièmement, **comment se donner les moyens de repérer effectivement ces biais, dont nous avons souligné le caractère parfois invisible ?** Faut-il d'ailleurs distinguer entre des biais qui seraient acceptables et d'autres que la société ne pourrait pas tolérer (comme ceux évoqués plus haut) ? Enfin, comment lutter efficacement contre ces biais et s'assurer que les algorithmes respectent les valeurs fondamentales élaborées démocratiquement par nos sociétés ?

Il faut enfin souligner ici une dimension que nous verrons resurgir dans la suite de ce rapport : les impacts non pas seulement individuels (sur la personne), mais également collectifs que peuvent avoir les algorithmes. L'exemple de l'exclusion par un service d'Amazon de quartiers entiers en offre une illustration.

Fragmentation algorithmique : la personnalisation contre les logiques collectives

L'omniprésence des algorithmes, notamment ceux liés à notre navigation sur le Web et sur les réseaux sociaux, est indissociablement liée à la dynamique de personnalisation des contenus et des services. Cette personnalisation au service de l'individu recèle cependant une dimension problématique en portant potentiellement atteinte à des logiques proprement collectives sur lesquelles reposent nos sociétés, de la structuration de l'espace public démocratique aux mécanismes de mutualisation dans l'ordre économique. Alors que l'impact des algorithmes sur les personnes est un phénomène bien repéré et pris en compte par la loi depuis longtemps, ses impacts collectifs posent également question aujourd'hui.

Enfermement algorithmique et perte de pluralisme culturel

Le thème de l'enfermement algorithmique a fait l'objet de nombreuses discussions depuis l'ouvrage d'Eli Pariser sur la « bulle filtrante[23] ». Il renvoie à l'idée selon laquelle l'activité indispensable jouée par les algorithmes en termes

22 Kate Crawford, "Artificial Intelligence's White Guy Problem", *The New York Times*, 25 juin 2016.
23 Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, New York, Penguin Press, 2011.

de classement et de filtrage d'une information devenue surabondante aurait pour effet indirect de nuire au pluralisme et à la diversité culturelle: en filtrant les informations, en s'appuyant sur les caractéristiques de leurs profils, **les algorithmes augmenteraient la propension des individus à ne fréquenter que des objets, des personnes, des opinions, des cultures conformes à leurs propres goûts et à rejeter l'inconnu.**

Le thème de la bulle filtrante se pose à deux échelles, celle des individus et celle de la société dans son ensemble.

À l'échelle de l'individu, le risque est que celui-ci se voie purement et simplement assimilé à un alter ego numérique constitué à partir de ses données et se trouve en quelque sorte enfermé dans une bulle de recommandations toujours conforme à ce profil. Les effets d'une offre culturelle et de contenus plus abondante que jamais auparavant se verraient ainsi paradoxalement neutralisés par un phénomène de limitation de l'exposition effective des individus à la diversité culturelle. Un tel phénomène pourrait d'ailleurs se produire alors même que l'individu souhaiterait en principe une telle diversité. La Direction Générale des Médias et des Industries Culturelles (DGMIC) souligne ainsi que « la recommandation algorithmique est fondée sur la consommation réelle des utilisateurs plutôt que sur leurs désirs ou aspirations ».

Il faut pourtant relever que d'importants spécialistes, chercheurs et praticiens du numérique contestent l'idée d'enfermement algorithmique ou du moins invitent à poser la question de manière plus nuancée. Ainsi, selon Antoinette Rouvroy, « cette question de la bulle filtrante n'est pas propre aux algorithmes: nous sommes des êtres très prévisibles, aux comportements très réguliers, facilitant la possibilité de nous enfermer dans des bulles. Mais on ne nous enferme que si c'est rentable. Tout est une question de paramétrage des algorithmes. Ils peuvent aussi, au contraire nous exposer à des éléments ou à des informations que nous n'aurions jamais cherché à consulter » (propos tenus le 23 janvier 2017 lors de l'événement de lancement du débat public à la CNIL). Il est vrai que l'on constate que cette potentialité n'est de fait guère exploitée. En effet, la consommation culturelle repose sur une structure duale de goûts : d'une part des liens forts « traduisant une préférence avérée pour un type de contenus bien identifié a priori », d'autre part des liens faibles « rendant compte d'une affinité non encore révélée pour un type de contenus restant à découvrir à posteriori[24] ». Or, la plupart des algorithmes prédictifs des grandes plateformes culturelles (Netflix, Amazon, Spotify, etc.) se focalisent sur les liens forts. Aucune des grandes catégories d'algorithmes n'envisage la sérendipité comme variable essentielle aux choix de consommation.

> Les algorithmes augmenteraient la propension des individus à ne fréquenter que des objets, des personnes, des opinions, des cultures conformes à leurs propres goûts et à rejeter l'inconnu

Dominique Cardon souligne quant à lui que « le numérique a apporté une diversité informationnelle jamais connue dans toute l'Histoire de l'Humanité. Il est absurde de dire que Facebook enferme les gens. Mais cela soulève des dangers : des gens curieux vont envoyer des signaux de curiosité et vont se voir incités en retour à la curiosité. En revanche, des gens donnant peu de traces de curiosité vont être dirigés vers moins de diversité. [...] Un risque existe que se produisent dans un certain contexte et pour un certain public, des pratiques sociales dans lesquelles l'algorithme ne sera pas un facteur d'enrichissement et de découverte, mais plutôt de reconduction du monde » (propos tenus le 23 janvier 2017 lors de l'événement de lancement du débat public à la CNIL). Enfin, la DGMIC estime que les incitations concurrentielles à la différenciation ainsi qu'*« une vision libérale de l'individu considérant l'étendue du choix comme un facteur d'épanouissement »*[25] pourraient limiter les risques pesant sur la diversité en incitant les acteurs à se saisir de l'enjeu de l'enfermement et à lui apporter des réponses.

À l'échelle de sociétés considérées dans leur ensemble, **les formes de privation d'exposition des individus à l'altérité, à des opinions différentes des leurs, notamment dans le registre politique, pourraient en tout cas constituer, selon certains, un problème pour la qualité et la vitalité du débat public, pour la qualité et la diversité de l'information, terreaux du fonctionnement correct des démocraties.**

À l'horizon logique du phénomène, la personnalisation de l'information aurait pour conséquence une fragmentation extrême de l'espace public, la disparition d'un socle minimum d'informations partagées par l'ensemble du corps politique et permettant la constitution d'un véritable débat.

24 Rapport du CSA Lab
25 Natali HELBERGER, Kari KARPPINEN & Lucia D'ACUNTO, "Exposure diversity as a design principle for recommender systems", Information, Communication & Society, 2016.

À l'heure où une part croissante des citoyens utilisent les réseaux sociaux comme le principal (et parfois seul) moyen d'information[26], l'enjeu est important pour la pérennité de la vie démocratique. Si la tendance à s'entourer de personnes partageant les mêmes idées et les mêmes valeurs n'est pas nouvelle, du moins la presse traditionnelle avec sa logique éditoriale permet-elle au lecteur d'avoir une plus claire conscience de l'orientation du contenu qu'il consomme. Les débats portant sur ce sujet font pourtant clairement ressortir que les effets dénoncés sous la rubrique de la « bulle de filtre » ne sont pas fatalement et toujours produits par les algorithmes. Ils sont avant tout le résultat du paramétrage d'algorithmes que l'on pourrait tout aussi bien programmer autrement et à qui l'on pourrait, à l'inverse, donner comme objectif d'exposer les individus à une diversité culturelle, informationnelle, politique forte.

Il est possible que la nature même du problème en ait ralenti la prise de conscience publique. À la limite, en effet, l'individu peut très bien vivre dans sa bulle informationnelle sans en prendre conscience. Le confort provoqué par l'absence de contradiction ou encore le biais de confirmation caractérisant l'esprit humain et que connaissent bien les sciences cognitives ne sont évidemment pas des facteurs propices à la remise en cause de l'enfermement algorithmique. Autrement dit, rien ne prédispose l'individu à s'apercevoir qu'il est pris dans une bulle informationnelle. Il n'est dès lors guère étonnant que les mises en cause de ce phénomène s'accompagnent souvent de récits relatant le moment de sa prise de conscience, un moment s'apparentant à un choc. C'est ainsi que les débats sur la bulle filtrante et ses effets politiques ont été notamment relancés à l'occasion de la campagne présidentielle américaine de 2016 ainsi que par celle du Brexit, quelques mois avant. Deux chocs électoraux à l'occasion desquels de nombreux internautes partisans d'Hillary Clinton ou opposants au Brexit ont été particulièrement frappés de constater des résultats que leurs fils d'actualité ne laissaient en rien présager. Plus récemment, en août 2017, la sociologue Zeynep Tufekci, spécialiste des mouvements de contestation en ligne a remarqué – parmi d'autres – que son fil d'information Facebook demeurait silencieux sur les événements de Ferguson au moment même où elle voyait le hashtag Ferguson se répandre sur Twitter.

On peut considérer que **l'absence de compréhension claire par les individus du fonctionnement des plateformes qu'ils utilisent pour s'informer, notamment, fait partie intégrante du problème.** Une étude a ainsi montré que plus de 60% des utilisateurs de Facebook n'ont aucune idée de l'activité éditoriale que joue effectivement l'algorithme et croient que tous les posts de leurs amis et des pages qu'ils suivent apparaissent sur leur fil d'actualités[27]. En vérité, ils n'en voient que 20%, sélectionnés selon plusieurs facteurs : promotion publicitaire du post, interactions passées de l'utilisateur avec des posts considérés comme similaires – *like,* commentaire, partage-, nombre d'autres utilisateurs ayant fait de même, etc.

L'usage fait des algorithmes par l'économie numérique à des fins de personnalisation du service et de l'expérience répond donc à une logique qui pose problème dès lors que l'on considère ses effets d'un point de vue, non plus seulement économique, mais aussi culturel ou politique. **L'objet des grandes plateformes algorithmiques est la satisfaction d'un consommateur, d'un *homo economicus*. Les effets politiques et culturels à grande échelle de leurs algorithmes ne leur posent question que secondairement.**

Atomisation de la communauté politique

Cet effet induit des algorithmes et de leur fonction de personnalisation peut néanmoins devenir un levier direct pour certains acteurs qui cherchent à les exploiter à des fins d'influence, voire de manipulation. Les *fake news,* largement évoquées lors de la campagne menée par Donald Trump, si elles ne sont pas un produit direct des algorithmes, se diffusent et s'amplifient à l'intérieur des chambres d'écho constituées par les algorithmes des réseaux sociaux ou des moteurs de recherche. Plus directement encore, des logiciels de stratégie politique de plus en plus élaborés et appuyés sur un ciblage de plus en plus fin des électeurs conduisent à une fragmentation potentiellement sans précédent d'un discours politique adressé désormais à des individus atomisés. Les pratiques de la société Cambridge Analytica, qui a travaillé pour le candidat Trump, représentent la pointe de diamant de ces nouveaux usages des algorithmes à des fins électorales (voir encadré). La tendance à la fragmentation personnalisée du discours politique, appuyée sur la capacité croissante de l'IA à composer des messages en fonction des différents profils, pose aujourd'hui de sérieuses questions. Faut-il y voir une forme de manipulation ? Faut-il y poser des limites ? Faut-il considérer ces pratiques comme le fruit inéluctable et difficilement régulable de l'évolution technologique et dès lors imaginer des contrepoids ? Si oui, lesquels ?

On le voit, le thème de l'enfermement est l'envers de celui de la personnalisation algorithmique. Ceci explique qu'enfermement et fragmentation puissent être aussi décelés dans des secteurs autres que celui de la consommation culturelle et des médias ou de la politique.

26 Selon le Pew Research Center, 61% des "millenials" utilisent Facebook comme leur première source d'information sur la politique l'action gouvernementale (Pew Research Center, *Millenials & Political News. Social Media – the Local TV for the Next Generation ?,* juin 2015).
27 http://www-personal.umich.edu/~csandvig/research/Eslami_Algorithms_CHI15.pdf

FOCUS

Algorithmes et stratégie électorale

Les dernières élections présidentielles, aux États-Unis mais aussi en France, ont donné lieu à l'utilisation croissante des **logiciels de stratégie électorale** reposant sur la mise en œuvre d'algorithmes prédictifs d'analyse des données électorales. Loin des méthodes plus traditionnelles de campagne, des messages politiques très ciblés peuvent désormais être adressés aux électeurs. C'est aux Etats-Unis que l'on peut identifier les exemples les plus accomplis d'un tel profilage individuel. Dès les élections présidentielles de 2008 et 2012, les équipes électorales de Barack Obama disposaient de centaines de données sur la quasi-totalité des électeurs. En 2016, grâce à l'analyse des données issues des réseaux sociaux et des courtiers en données, Cambridge Analytica aurait pu envoyer pour le compte du candidat Trump des milliers de messages extrêmement individualisés au cours d'une même soirée[28]. Si cette entreprise a par la suite tenu un discours tendant à minimiser ses premières affirmations, cette affaire n'en est pas moins révélatrice d'une tendance de fond susceptible de s'approfondir à l'avenir.

En France, les **principes de protection des données à caractère personnel** limitent toutefois dans les faits le développement de tels logiciels de ciblage individuel, le consentement constituant un prérequis essentiel à une telle collecte. La CNIL a d'ailleurs rappelé, dans un communiqué de novembre 2016, les règles pour l'utilisation des données issues des réseaux sociaux à des fins de communication politique[29].

L'enfermement algorithmique, un enjeu transversal

La question de l'enfermement algorithmique ne se limite pas aux secteurs de la culture, de l'information ou de la politique. En effet, l'intrication des fonctions de prédiction et de recommandation présentes dans les usages des systèmes algorithmiques aujourd'hui modelés par l'écosystème numérique est susceptible de générer des prophéties auto-réalisatrices pouvant enfermer les individus dans un destin « prédit ».

Une forme d'enfermement n'est-elle pas une conséquence possible de futurs usages des *learning analytics* et de l'*adaptative learning* (ou éducation personnalisée) ? Sans remettre en cause les promesses de ces techniques, il est légitime de s'interroger sur les effets que pourraient avoir des systèmes prétendant définir des parcours d'apprentissage sur la base du profil de chaque élève et de la prédiction élaborée à partir de l'application d'un modèle mathématique à ce profil. N'y a-t-il pas un risque que la prédiction devienne auto-réalisatrice et que l'élève se trouve assigné à un destin scolaire et professionnel dès lors que le diagnostic aura été posé ? Comme le souligne Roger-François Gauthier, « avec les *learning analytics,* la prédiction pourrait déboucher sur un enfermement des élèves. En France, ce genre de problème suscite trop peu d'attention. Il faut pourtant faire en sorte que l'élève échappe au déterminisme et pour cela la question des valeurs inscrites dans les systèmes algorithmiques est fondamentale[30] ».

On peut, de la même façon, rattacher à l'idée d'enfermement algorithmique certains impacts possibles de l'utilisation des algorithmes dans le secteur des ressources humaines et du recrutement. Laurence Devillers évoque ainsi le risque de « normalisation des profils » que pourrait faire courir l'algorithme, du moins un usage non raisonné de l'algorithme, au recruteur. C'est en quelque sorte ce dernier qui serait victime ici d'enfermement dans des profils prédéfinis à l'avance, se privant de la part de sérendipité inhérente au processus de recrutement dans la mesure où celui-ci peut permettre de repérer des profils atypiques, non conformes aux critères définis *a priori,* mais finalement intéressants. Comment repérer de tels profils si une part croissante de la sélection des candidats se trouve déléguée à des systèmes automatiques ?

28 https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage
29 https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux
30 Propos tenus à l'occasion du lancement du débat public, le 23 janvier 2017, à la CNIL.

Démutualisation

La personnalisation algorithmique soulève un enjeu spécifique au secteur de l'assurance. En effet, **la dynamique de personnalisation des offres et des services ne conduit-elle pas à une remise en cause de la mutualisation, c'est-à-dire de la logique même de l'assurance et du pacte social sur lequel elle repose ?** Que plusieurs individus acceptent de s'assurer, c'est-à-dire de mettre en commun leurs risques, suppose que ces risques leur demeurent au moins partiellement opaques. Je m'assure en ignorant lequel de moi ou de mon voisin contractera une maladie occasionnant de lourds frais de santé. La segmentation accrue que rendrait possible l'utilisation des masses de données générées par les comportements des individus en ligne (réseaux sociaux, notamment) ou hors-ligne (données issues de bracelets connectés, par exemple) tendrait à lever le « voile d'ignorance[31] » sous-tendant la mutualisation assurantielle et que contribue à maintenir une segmentation sommaire.

Ces innovations ne déboucheront-elles pas sur de nouvelles formes de discrimination et d'exclusion ? Les individus jugés « à risque » pourraient se voir appliquer des tarifs plus élevés, voire même être victimes de décisions de refus d'assurance. À cela s'ajoute le fait que l'établissement d'une corrélation entre un comportement et le risque de survenue d'une pathologie pourrait aboutir à défavoriser les individus ayant des comportements jugés « à risque » (consommation de tabac, nourriture jugée trop grasse, trop sucrée, etc.). La question serait alors celle des limites à poser à ce qui peut apparaître comme une normalisation excessive des comportements des personnes lorsque ceux-ci seraient estimés « mauvais ». Les algorithmes, via les corrélations qu'ils établissent dans les données, finiraient par édicter la norme des comportements individuels, une norme à laquelle on ne pourrait échapper qu'au prix d'un renchérissement de l'assurance. À la différence d'un mécanisme comme l'augmentation des prix du tabac (dont la consommation est considérée comme un coût pour la collectivité), de tels arbitrages échapperaient à la délibération collective et surgiraient des données mêmes. Par ailleurs, une telle approche évacuerait complètement les déterminants collectifs et sociaux des comportements pour ne plus mettre en exergue que la seule responsabilité des individus. Quant à d'autres facteurs de risque, liés à l'environnement de l'individu ou à son patrimoine génétique, ils seraient susceptibles de déboucher sur une discrimination et une exclusion inévitables dans la mesure où les personnes concernées n'auraient aucune prise sur eux.

Si la course aux « bons risques » pourrait donc être accrue entre les assureurs, il est cependant douteux que celle-ci soit favorable à ces derniers pris dans leur ensemble. L'assureur aurait intérêt à la mutualisation. Selon Florence Picard, de l'Institut des Actuaires, *« plus il segmente fermement les groupes, plus il prend le risque de mettre fin à la mutualisation. Son but est que le risque soit maîtrisable: plus on segmente, plus on prend le risque de se tromper[32] ».*

Entre limitation des mégafichiers et développement de l'intelligence artificielle : un équilibre à réinventer

Le fonctionnement des algorithmes auxquels nous avons quotidiennement recours repose sur le traitement de nombreuses données, dont une grande part de données personnelles, traces numériques laissées par nos navigations en ligne, par l'utilisation de nos smartphones, de nos cartes de crédit, etc. **La recherche d'une performance accrue des algorithmes est un facteur allant dans le sens d'une collecte croissante, d'un traitement et d'une conservation accrus de données à caractère personnel.**

On peut ainsi se demander si le développement de l'intelligence artificielle n'est pas susceptible, à un certain stade, d'entrer en tension avec les principes éthiques inscrits dans la législation depuis la loi Informatique et libertés. L'intelligence artificielle est grande consommatrice de données ; elle a besoin d'une grande mémoire (autrement dit, de bases de données qu'elle va conserver sur une période aussi longue que possible). Les principes de la loi de 1978 renvoient, quant à eux, par le truchement du principe de finalité, à une minimisation de la collecte de données per-

31 Antoinette Rouvroy déplace ainsi, en l'appliquant au domaine de l'assurance, le concept forgé par John Rawls pour établir une expérience de pensée destinée à envisager un problème moral.

32 « Algorithmes et risques de discriminations dans le secteur de l'assurance », manifestation organisée par la Ligue des Droits de l'Homme le 15 septembre 2017.

sonnelles ainsi qu'à la limitation de la durée de conservation de ces données comme à des garanties nécessaires à la protection des personnes et de leurs libertés.

Certes, les principes de la loi de 1978 (repris dans le Règlement général sur la protection des données, qui entrera en application en mai 2018) constituent un équilibre général, offrant une certaine souplesse à l'ensemble. Des mesures de sécurité renforcées peuvent dans une certaine mesure être considérées comme un contrepoids à une durée de conservation allongée des données. Il n'est pourtant pas certain que l'ampleur des transformations technologiques induites par le développement de l'intelligence artificielle ne remette pas en cause ce schéma.

Par exemple, la médecine de précision semble lier ses progrès à la constitution de bases de données toujours plus larges, à la fois en termes de nombres d'individus concernés qu'en termes de nombre et de variété de données conservées sur chacun d'entre eux. L'épigénétique prétend ainsi croiser une approche par les données génétiques de l'individu à une approche prenant en compte les données environnementales, celles concernant le milieu, voire le mode de vie du « patient » (si tant est que cette notion ait encore un sens dans un contexte de plus en plus orienté vers la « prédiction »). La médecine de précision repose sur l'idée de profiler le plus finement possible ce dernier et la pathologie dont il est affecté afin de comparer ce profil à ceux d'autres individus au profil très proche, de façon à identifier le traitement le plus approprié à ce patient. À la limite, on pourrait aller jusqu'à considérer que l'objectif sanitaire poursuivi implique la constitution d'immenses bases de données. Or, rien n'indique où devrait s'arrêter la collecte de données : au dossier médical ? Au génome ? Aux données épigénétiques, c'est-à-dire environnementales (habitudes de vie, habitat, alimentation, etc.) ? En remontant à combien d'années ? Notons que ce type de problème n'est nullement propre à la médecine. Il se poserait sous un aspect proche dans le domaine de la sécurité, où l'impératif de repérage des suspects semble justifier une collecte de données toujours plus massives sur les individus.

On voit bien que **la question posée ici est celle de l'équilibre à trouver entre protection des libertés (protection des données personnelles) et progrès médicaux.** Il ne saurait être question d'y répondre ici, tant elle mériterait de faire l'objet d'une réflexion poussée. Celle-ci devrait d'ailleurs nécessairement impliquer une évaluation des progrès effectivement à attendre de la médecine de précision. Ainsi Philippe Besse, professeur de mathématiques à l'Université de Toulouse, considère que les données mises à la disposition de la recherche médicale dans le cadre du Système National des Données de Santé (SNDS) sont suffisantes pour accomplir des progrès que la complexité du vivant limitera de toute façon bien en-deçà de ce qu'annoncent certaines prophéties[33].

Qualité, quantité, pertinence : l'enjeu des données fournies à l'IA

Les systèmes algorithmiques et l'intelligence artificielle reposent sur l'utilisation de données (personnelles ou non) qui leur sont fournies en entrée et qu'ils traitent pour produire un résultat. Schématiquement, cette caractéristique soulève trois enjeux connexes mais distincts : celui de la qualité, celui de la quantité et celui de la pertinence des données fournies à ces systèmes.

La **question de la qualité des données utilisées par les algorithmes et l'IA** est la plus simple. Il est facile de comprendre que **des données erronées ou tout simplement périmées impliqueront en bout de chaîne des erreurs ou des dysfonctionnements plus ou moins graves selon le domaine concerné,** du simple envoi de publicités ciblées correspondant mal à mon profil réel jusqu'à une erreur de diagnostic médical. Assurer la qualité de la donnée entrante dans les systèmes algorithmiques et d'intelligence artificielle constitue donc un enjeu appelé à prendre une importance de plus en plus cruciale au fur et à mesure que ces machines vont être amenées à prendre une autonomie croissante. Or, assurer la qualité de la donnée est coûteux. La corruption des données peut être le résultat aussi bien d'un problème technique très matériel impliquant l'état des capteurs affectés à leurs collecte que d'un problème humain lié à l'intérêt de certains acteurs à biaiser les données qu'ils sont chargés d'entrer dans le système. La tentation de la négligence à cet égard doit être prise au sérieux, notamment dans des domaines où l'impact de données de

33 Débat organisé par le Génotoul à Toulouse, le 24 juin 2017.

mauvaise qualité pourrait n'être pas immédiatement sensible, comme dans le secteur du recrutement, par exemple. Les données des réseaux sociaux professionnels, parfois considérées comme une manne inépuisable, posent à cet égard des problèmes de fiabilité (liés à la tendance des individus à embellir leur CV ou au contraire à des absences de mise à jour). La confiance accordée par l'utilisateur au résultat produit par une machine jugée objective et plus performante que l'homme est un facteur supplémentaire pouvant favoriser la négligence.

La **quantité de données disponibles** peut constituer un autre facteur néfaste à la qualité des résultats fournis par les systèmes algorithmiques et d'intelligence artificielle. Cathy O'Neil évoque ainsi l'exemple d'une collectivité ayant recouru aux États-Unis à un logiciel d'évaluation des enseignants. L'utilisation de ce logiciel s'est notamment soldée par le licenciement d'enseignants dont la qualité était pourtant de notoriété publique dans les communautés locales au sein desquelles ils évoluaient. L'une des raisons essentielles en est que l'algorithme utilisé pour évaluer la progression annuelle des élèves de chaque enseignant aurait besoin de bien plus que des données concernant tout au plus quelques dizaines d'élèves. Dans un cas où les variables susceptibles d'expliquer, à côté de la performance du professeur, les mauvais résultats d'un élève (difficultés relationnelles, problèmes familiaux, problèmes de santé, etc) sont si nombreuses, un nombre si limité de cas ne peut avoir aucune valeur statistique. La seule valeur de ce résultat est de donner le sentiment aux décideurs de prendre des décisions rationnelles, objectives et efficaces car s'autorisant du prestige de la machine.

Cela ne signifie toutefois nullement que l'accumulation irréfléchie de données doive constituer un objectif en soi. Dans certains cas, en effet, la variété des données sera plus précieuse que leur simple quantité. Par exemple, les données de millions de véhicules suivant la même route seront moins utiles à l'algorithme d'une application GPS que des données en bien moins grand nombre de véhicules empruntant des itinéraires plus variés.

Enfin, **la question de la pertinence des données renvoie moins à la véracité de ces dernières qu'aux biais qui peuvent présider à leur collecte.** Comme cela a été montré précédemment (Voir « Biais, discriminations et exclusion »), il peut être tout à fait exact que très peu de femmes aient mené à bien une carrière de haut niveau dans telle ou telle entreprise. En revanche, prendre ce résultat comme indicatif de la capacité de femmes à accomplir à l'avenir de brillantes carrières dans cette même entreprise relève bien évidemment d'une approche biaisée. En l'occurrence, le jeu de données envisagé ici intègre des formes d'inégalités et/ou de discriminations. Ignorer ce type de biais reviendrait à perpétuer ou à laisser se perpétuer ces phénomènes.

On voit à travers ces trois enjeux que les promesses des algorithmes ne peuvent être tenues qu'au prix d'une grande rigueur dans la collecte et le traitement des données utilisées. Qu'une telle exigence de rigueur (et d'investissement matériel et humain) puisse ne pas être respectée par certains acteurs représente un risque évident, alors même que les algorithmes sont souvent présentés comme sources d'une vérité « objective », « neutre ». Dans l'exemple de l'algorithme utilisé pour évaluer les professeurs aux États-Unis évoqué par Cathy O'Neil, **la négligence méthodologique des concepteurs et promoteurs de l'algorithme a pour corollaire la confiance exagérée, dénuée d'esprit critique** qu'accordent à ce dernier des utilisateurs dont l'attention se focalise sur la seule nécessité d'obtenir un quota de professeurs à éliminer du système. Pourtant, si assurer la qualité et la pertinence des données fournies aux algorithmes s'impose donc comme une exigence éthique, cette dernière constitue bien à terme une condition de l'utilité durable des algorithmes pour leurs utilisateurs et pour la société en général.

ENQUÊTE

La crainte devant les risques des algorithmes et de l'IA augmente avec l'âge*

Les jeunes sont plus sensibles aux opportunités portées par l'algorithme : 68,5 % des 18-24 ans considèrent que les opportunités surpassent les potentielles menaces. En revanche, seul 36 % des 55-64 ans estiment que les bénéfices sont plus importants que les risques.
Certaines applications des algorithmes sont mieux acceptées chez les plus jeunes: 75 % des 18-24 ans regardent favorablement des recommandations en vue d'achats en ligne (contre 48 % pour l'ensemble du panel), 50 % en vue du choix de l'âme-sœur (contre 26 %).

* Enquête réalisée dans le cadre du débat public par l'association « Familles rurales », association familiale orientée vers les milieux ruraux, auprès de 1076 de ses adhérents.

L'identité humaine au défi de l'intelligence artificielle

L'autonomisation des machines, d'une part, l'hybridation croissante des humains avec la machine, d'autre part, questionnent l'idée d'une spécificité humaine irréductible.

Des machines éthiques ?

La première zone de porosité entre humains et machines s'établit autour de la question de l'idée de machine éthique. En effet, une façon radicale d'aborder les questions soulevées par l'éventuelle délégation de décisions à des machines autonomes (intelligence artificielle) est d'envisager que de rendre les machines « éthiques » serait une solution aux problèmes évoqués plus haut dans ce rapport. Une telle piste de réflexion est liée à la question de savoir s'il est même possible de formaliser une éthique[34] afin de la programmer dans une machine. Autrement dit, **peut-on automatiser l'éthique ?** Ce problème est apparu au cours des débats comme l'un de ceux retenant particulièrement l'attention de la communauté des chercheurs en intelligence artificielle. Gilles Dowek (CERNA) l'a ainsi souligné lors de la journée d'étude organisée au Collège des Bernardins le 20 septembre 2017.

Le fameux dilemme du tramway est très souvent évoqué à l'occasion de réflexions portant sur ce problème. On sait que ce dilemme met en scène un tramway sans freins dévalant une pente ; le tramway arrive devant un embranchement ; selon qu'il s'engage sur l'une ou l'autre des deux voies, il tuera une personne ou bien plusieurs. Dès lors, quelle devrait être la conduite d'une personne ayant la possibilité de manœuvrer l'aiguillage et donc de choisir, pour ainsi dire, l'un des deux scénarios possibles ? L'intérêt de cette expérience de pensée est qu'elle peut donner lieu à toute une gamme de variations : qu'en est-il si la personne seule attachée à l'une des deux voies se trouve être un proche parent ? Si les personnes sur l'autre voie se trouvent être 5 ou bien 100 ?

On voit aisément comment ce dilemme peut être adapté à l'hypothèse de voitures autonomes qui seraient mises en circulation prochainement : selon quels principes une voiture placée dans une situation de dilemme éthique de ce type devrait-elle « choisir » de se comporter ? Le dilemme du tramway a l'intérêt de mettre en évidence le fait que différents choix « éthiques » sont possibles. Dès lors que des dilemmes de ce type auraient été anticipés au stade du développement du système, il serait bien sûr possible de leur donner une réponse. Mais précisément, **la spécificité de l'éthique n'est-elle pas de concerner des situations inédites, impliquant éventuellement des conflits de valeurs dont la solution doit être élaborée par le sujet** (pensons à Antigone, prise entre éthique familiale et éthique civique) ? N'est-elle pas de s'élaborer toujours en situation ? Dès lors l'hypothèse d'une formalisation de l'éthique n'est-elle pas quelque peu illusoire ? À tout le moins, elle implique une conception implicite de l'homme qui n'a rien d'évident.

Retenons du moins que, pour l'heure, des expressions comme « éthique des algorithmes » ou « algorithmes éthiques » ne doivent pas être prises au pied de la lettre et comportent une part d'anthropomorphisme revenant à attribuer des capacités humaines à des machines. Certains considèrent qu'elles sont susceptibles de fausser un débat qui devrait se concentrer sur les exigences à l'égard des hommes qui conçoivent, entraînent, déploient et utilisent les systèmes algorithmiques et d'intelligence artificielle.

Elles ne constitueraient alors qu'une métaphore commode mais à ne pas entendre littéralement. À l'inverse, comme le rappelle par exemple Gilles Dowek, on peut considérer comme légitime le recours à ce type de métaphores dans la mesure où elles reviennent à prendre acte de l'autonomie croissante de ces systèmes et de la nécessité de formaliser, autant que faire se peut, une éthique et de la programmer dans des algorithmes. Quoi qu'il en soit, même si une éthique en tant que telle pouvait être encodée dans une machine (c'est-à-dire si cette dernière avait la possibilité de ne pas seulement répondre d'une certaine façon à une situation éthique envisagée à l'avance lors de son développement mais bien d'aborder des situations nouvelles en leur appliquant un raisonnement éthique), le choix du type d'éthique à encoder resterait bien, en dernière analyse, du ressort de l'homme. Le vrai enjeu est alors de s'assurer que les choix éthiques faits au stade du développement ne font pas l'objet d'une confiscation par « une petite caste de scribes » (Antoine Garapon). L'échelle de déploiement des algorithmes à l'heure du numérique en fait une question démocratique essentielle.

34 C'est-à-dire une règle générale d'évaluation de la conduite à adopter face à toute situation – éthique déontique ou éthique conséquentialiste – ou un corpus de règles remplissant la même fonction – éthique kantienne, éthique bouddhiste, etc.

L'hybridation de l'homme et de la machine : repenser l'identité humaine ?

Une façon d'envisager la question éthique appliquée aux algorithmes et à l'intelligence artificielle peut être de confronter ces derniers à l'affirmation – présente à l'article premier de la loi Informatique et libertés – selon laquelle l'informatique « ne doit pas porter atteinte à l'identité humaine ».

Les pages précédentes ont abordé des problèmes liés à la façon dont l'homme agence son action avec des artefacts, question ancienne mais renouvelée par l'émergence d'artefacts dotés d'une « autonomie » croissante à l'heure des algorithmes et de l'intelligence artificielle[35]. Ces propos soulignent en effet que le développement de ces technologies, selon la manière dont il s'opérera, peut affecter l'une des composantes de l'identité et de la dignité humaines, à savoir sa liberté et sa responsabilité. La montée en puissance d'une forme d' « autonomie » machinique doit bien sûr être fortement nuancée. Gérard Berry, professeur au Collège de France et titulaire de la chaire « Algorithmes, machines et langages » rappelle ainsi : « un jour, nous dit-on, les machines parleront et seront autonomes, le numérique donnera naissance à une nouvelle forme de vie. La date pour l'autonomie des machines et leur capacité de parole créative, personne ne la donne, et je ne la connais pas, loin de là. Surtout, de quelle vie parlons-nous ?[36] ». Néanmoins, on pourrait se demander si la trajectoire technologique d'ores et déjà à l'œuvre ne devra pas conduire à questionner la pertinence de la notion même d' « identité humaine », dans la mesure où celle-ci implique une séparation étanche entre humain et non-humain. La question du « droit des robots » d'ores et déjà soulevée par des juristes et récemment examinée par le Parlement européen (rapport Delvaux) a pour horizon ce brouillage possible des frontières de l'humain. À de tels arguments post-humanistes, la tradition humaniste pourrait certes rétorquer que l'autonomie machinique n'est aujourd'hui qu'un leurre, une métaphore destinée à styliser un objet complexe et masquant finalement une responsabilité et une action humaines certes diluées, éclatées, mais bien réelles.

> Le développement de ces technologies peut affecter l'une des composantes de l'identité et de la dignité humaines, à savoir sa liberté et sa responsabilité

Si une première hybridation entre l'homme et la machine s'opère au plan de l'action, la réflexion devra aussi nécessairement s'élargir à l'avenir pour prendre en compte l'hybridation physique parfois annoncée entre algorithmes, humains, voire animaux (avec l'adjonction d'implants intelligents et communicants). Cette hybridation physique est une étape supplémentaire de l'évolution déjà à l'œuvre dans l'interaction permanente qui nous lie d'ores et déjà à une foule de processus algorithmiques.

Enfin, ce thème d'une subversion éventuelle de la frontière entre l'homme et les choses (ou plutôt, entre l'homme et la machine) trouve déjà une réalité extrêmement concrète au plan phénoménologique dans certaines tentatives récentes d'applications de la robotique qui s'illustrent d'abord dans la forme humaine donnée aux robots. On pense ici au robot Pepper de la firme Aldebaran, destiné à être déployé dans des espaces commerciaux pour interagir avec les clients. Surtout, et ceci concerne directement le sujet des algorithmes et de l'intelligence artificielle, **tout un champ de recherche vise à créer des robots empathiques capables de percevoir les émotions des humains** (par l'analyse du visage, de la voix, etc.) de façon à s'adapter à leur interlocuteur. La première question posée par ces recherches est évidemment celle de la limite entre, d'une part, les apports bénéfiques d'une intelligence artificielle capable de comprendre et de s'adapter aux états émotionnels de ses interlocuteurs et, d'autre part, une forme de manipulation appuyée sur une ingénierie technique capable d'exploiter les vulnérabilités affectives des personnes[37]. La seconde question, connexe à la première, est celle de savoir dans quelle mesure la capacité d'illusion propre à ces technologies et l'asymétrie qui existera entre ces robots et les personnes dont ils analyseront les émotions les rendent moralement acceptables ? Sherry Turckle, professeure au MIT, souligne ainsi que les êtres humains ont une grande propension à attribuer aux robots une subjectivité et une sensibilité[38]. Or, la tentation est forte pour des sociétés vieillissantes de confier de plus en plus le soin des personnes âgées à ce type de robots. En France, Serge Tisseron développe une réflexion critique sur ces technologies[39] . Quelles que soient les réponses apportées à ces questions, il semble essentiel qu'elles n'occultent nullement la dimension politique et de choix de société que recèle le fait de recourir aux robots plutôt que d'investir dans d'autres types de ressources (temps, ressources en personnel, etc.) pour l'accompagnement des membres vulnérables de nos sociétés.

35 La question de l'hybridation entre l'homme et des artefacts n'est pas nouvelle : les algorithmes participent au modelage de notre identité de la même façon que – Socrate le remarquait déjà dans le *Phèdre* de Platon – l'écriture affecte notre capacité de mémorisation et constitue un artefact muet, incapable de la moindre explication. Que l'idée d'une « identité humaine » strictement distincte des objets soit remise en cause n'implique ainsi pas nécessairement une nouveauté radicale.
36 Gérard Berry, « Non, l'intelligence artificielle ne menace pas l'humanité ! », interview donnée au Point, 18 mai 2015.
37 Une problématique très similaire à celle soulevée par les logiciels de communication politique censés adapter le message du candidat aux attentes de chaque individu ciblé et profilé.
38 Sherry Turckle, *Seuls ensemble,* Paris, L'Echappée, 2015 [2012].
39 Serge Tisseron, *Le Jour où mon robot m'aimera. Vers l'empathie artificielle,* Paris, 2015.

Quelles réponses ?

Quelles réponses ?

De la réflexion éthique à la régulation des algorithmes

Faut-il réguler les algorithmes ?

La question se trouve depuis quelques mois fréquemment évoquée aussi bien dans la presse généraliste que parmi les experts du numérique et des politiques publiques.
Elle ne constitue que le prolongement de la question de la régulation du numérique lui-même. On le sait, l'univers numérique s'est constitué en partie en opposition à l'idée même de normes, du moins de normes juridiques. De la contre-culture américaine des années 1960 à la mise en avant par les entreprises numériques de la nécessité de ne pas entraver l'innovation par un système de normes inadaptées à un univers fondamentalement nouveau, cette méfiance à l'égard de la régulation trace comme un fil rouge. Ce courant de pensée a trouvé une de ses manifestations les plus claires dans la fameuse Déclaration d'indépendance du cyberespace de John Perry Barlow en 1996. Il se heurte depuis de nombreuses années aux efforts déployés par les acteurs étatiques pour soumettre l'univers numérique au droit commun, parfois de manière mécanique, parfois en mettant en œuvre de véritables innovations juridiques.

De nombreux acteurs expriment aujourd'hui l'idée qu'il ne faudrait pas réguler les algorithmes et l'intelligence artificielle. Ces derniers soulignent en effet qu'il serait trop tôt pour imposer des règles qui s'avéreraient nécessairement inadaptées et vouées à être rendues rapidement caduques par des évolutions techniques progressant désormais à un rythme incommensurable à celui de l'invention juridique.

Une telle position néglige à vrai dire une réalité juridique aussi massive que parfois inaperçue : **les algorithmes et leurs usages se trouvent d'ores et déjà encadrés, directement ou indirectement, par de nombreuses règles juridiques.** Il est vrai que ces règles, comme on le verra, se trouvent en fait dispersées dans divers lois et codes, à la mesure de la transversalité du numérique.

Par ailleurs, des sondages effectués à l'occasion du débat public initié par la CNIL ont mis en évidence une attente de règles et de limites en matière d'algorithmes et d'intelligence artificielle. Ces règles et ces limites peuvent être conçues autrement que comme des normes contraignantes, par exemple sous la forme de « chartes » adoptées par une entreprise, par une profession, par une branche. C'est ce que montre par exemple le sondage réalisé par la CFE-CGC auprès de 1263 de ses adhérents[40].

La création par le Parlement d'une mission de réflexion confiée à la CNIL sur les enjeux éthiques et de société soulevés par l'évolution des technologies numériques s'inscrit dans ce contexte. Elle traduit évidemment un souci de réflexion sur les limites, sur les normes – quelle que soit la nature de ces dernières – à imposer à des nouveautés techniques. Elle traduit tout autant une volonté de la part de la puissance publique de ne pas céder à la tentation de réguler trop vite et de manière inadaptée. À cet égard, considérer que l'émergence et la diffusion de technologies nouvelles implique une réflexion sur ses limites ne signifie nullement que la loi soit systématiquement la forme adaptée à l'imposition de ces limites. C'est en tout cas ce qu'a considéré la CNIL en souhaitant ouvrir la réflexion de la façon la plus large possible, non seulement aux acteurs publics mais aussi aux praticiens, professionnels et grand public.

Formuler des recommandations impliquait donc d'abord d'explorer les grands développements des innovations considérées et les enjeux éthiques et de société soulevés par ceux-ci. Les pages précédentes y ont été consacrées. Les pages suivantes viseront à faire le point sur les grands principes susceptibles de répondre à ces enjeux ainsi que sur les recommandations concrètes envisageables aujourd'hui.

40 À la question « La définition d'une charte éthique autour de l'usage des algorithmes dans le recrutement et la gestion RH vous semble-t-elle une priorité ? », 92% ont répondu positivement.

Ce que la loi dit déjà sur les algorithmes et l'intelligence artificielle

Tous les défis identifiés dans le présent rapport ne sont pas nouveaux.

La Commission Tricot, dont le rapport a constitué la base de la loi de 1978 sur la protection des données à caractère personnel, en avait déjà identifié certains à l'issue d'une réflexion qui, au-delà du traitement des données, portait sur les défis soulevés par l'informatisation de l'État et de la société française. Le risque de discrimination ou d'exclusion des personnes mais également le risque d'une confiance excessive accordée à l'ordinateur étaient d'emblée clairement identifiés, à côté des enjeux directement liés à la capacité de collecter et de stocker de grandes quantités de données. Les débats portant sur la nécessité ou non de « réguler les algorithmes » ignorent en fait purement et simplement le fait que les algorithmes sont encadrés par la loi (loi Informatique et Libertés, notamment, mais pas seulement) depuis une quarantaine d'années.

> Les débats portant sur la nécessité ou non de « réguler les algorithmes » ignorent le fait que les algorithmes sont encadrés par la loi depuis une quarantaine d'années

Aboutissement du travail de la Commission Tricot, la loi Informatique et Libertés de 1978 contient en effet un certain nombre de dispositions que l'on peut, de façon schématique, rattacher à trois principes, eux-mêmes abrités sous un principe général contenu dans l'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 ».

Ces trois principes se trouvent relayés dans le Règlement européen sur la protection des données personnelles (RGPD) entrant en vigueur en mai 2018. Ils sont les suivants :

Premièrement, la loi encadre l'utilisation des données personnelles nécessaires au fonctionnement des algorithmes, au-delà même du traitement algorithmique à proprement parler. Autrement dit, elle encadre les conditions de collecte et de conservation des données[41], ainsi que l'exercice de leurs droits par les personnes (droit à l'information, droit d'opposition, droit d'accès, droit de rectification) afin de protéger leur vie privée et leurs libertés.

Deuxièmement, la loi Informatique et Libertés interdit qu'une machine puisse prendre seule (sans intervention humaine) des décisions emportant des conséquences cruciales pour les personnes (décision judiciaire, décision d'octroi de crédit, par exemple)[42].

Troisièmement, la loi prévoit le droit pour les personnes d'obtenir, auprès de celui qui en responsable, des informations sur la logique de fonctionnement de l'algorithme[43].

Au-delà de la loi Informatique et Libertés, d'autres dispositions légales plus anciennes constituent de fait un cadre et une série de limites à l'utilisation des algorithmes dans certains secteurs, dans la mesure même où ils régulent ces secteurs[44]. La question de la collusion algorithmique qui se pose aujourd'hui aux régulateurs de la concurrence, par exemple, ne se pose pas dans un vide juridique : elle a plutôt trait à l'effectivité de la règle de droit et à la nécessité d'inventer de nouveaux moyens de prouver l'existence d'ententes illégales[45].

Les dispositions juridiques interdisant différentes formes de discrimination, élaborées dans le sillage de l'article 7 de la Déclaration universelle des droits de l'homme, s'appliquent naturellement aux algorithmes[46].

41 Principes de finalité, de proportionnalité, de sécurité, de limitation de la durée de conservation des données.
42 Article 10 de la loi de 1978. Article 22 du RGPD.
43 Article 39 de la loi de 1978. L'article 15.1 (h) du Règlement européen sur la protection des données personnelles (RGPD) prévoit que la personne peut obtenir du responsable de traitement des informations concernant "the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject". Les limites juridiques posées par le RGPD portent notamment sur « le profilage » (pas de décision basée uniquement sur un traitement sauf exceptions).
44 On pourrait envisager, en forçant un peu le raisonnement, l'application du code de la santé publique (qui réprime l'exercice illégal de la médecine par toute personne non titulaire d'un diplôme) à des dispositifs d'intelligence artificielle dans le domaine médical. On pourrait imaginer qu'une telle disposition aussi puisse fonder l'interdiction de l'établissement d'un diagnostic par un algorithme seul. L'origine de cette législation, au début du XIXe siècle, renvoie à la préoccupation des autorités de lutter contre le « charlatanisme ». Les critiques des promesses excessives portées par certaines entreprises y verront sans doute un écho plaisant à la situation actuelle.
45 http://internetactu.blog.lemonde.fr/2017/02/11/comment-prouver-les-pratiques-anticoncurrentielles-a-lheure-de-leur-optimisation-algorithmique/
46 « Tous sont égaux devant la loi et ont droit sans distinction à une égale protection de la loi. Tous ont droit à une protection égale contre toute discrimination qui violerait la présente Déclaration et contre toute provocation à une telle discrimination ».

Les limites de l'encadrement juridique actuel

Un certain nombre des enjeux soulevés par les algorithmes constituent cependant à ce jour un angle mort du droit et des différentes dispositions juridiques évoquées précédemment.

Focalisation sur les algorithmes traitant des données personnelles et absence de prise en compte des effets collectifs des algorithmes

En premier lieu **ces dispositions ne concernent les algorithmes que dans la mesure où ils utilisent pour fonctionner des données à caractère personnel** et où leurs résultats s'appliquent directement à des personnes. C'est notamment le cas de la loi Informatique et libertés, la seule parmi celles évoquées qui vise directement les algorithmes (mentionnés comme « traitement automatisés de données à caractère personnel »). Or, bien des algorithmes n'utilisent pas de données à caractère personnel. C'est par exemple le cas des algorithmes boursiers. Les impacts de ces algorithmes traitant des données non personnelles sont tout aussi susceptibles que les autres de soulever des questions. Si les algorithmes boursiers relèvent d'un secteur par ailleurs fortement encadré, d'autres exemples peuvent permettre de comprendre les impacts que peuvent avoir des algorithmes ne traitant pas des données à caractère personnel. Celui, déjà évoqué au début de ce rapport (Voir « Une question d'échelle : la délégation massive de décisions non critiques »), de l'algorithme imaginé par Cathy O'Neil pour composer les repas de ses enfants lui permet de mettre en lumière les enjeux spécifiques liés à l'échelle de l'impact des algorithmes exécutés par des systèmes informatiques. On pourrait imaginer également un algorithme établissant les menus des cantines scolaires selon certains critères (optimisation du coût des denrées, qualité nutritionnelle, etc.) et qui pourrait être utilisé à l'échelle d'un pays. Un tel algorithme, sans traiter de données personnelles, serait susceptible d'avoir des impacts sociaux et économiques du fait même de son échelle de déploiement. Or, la loi n'a jusqu'ici pas pris en compte cette dimension nouvelle.

En second lieu, **les dispositions légales évoquées précédemment concernent les effets des algorithmes sur les personnes, dans une perspective individualiste. En revanche, elles ne visent pas directement leurs effets sur des collectifs.** Nous pensons ici par exemple aux impacts des algorithmes utilisés à des fins de marketing électoral sur le fonctionnement démocratique même (Voir : « Atomisation de la communauté politique »). Si l'on peut considérer que la loi Informatique et libertés constitue de fait un facteur limitant de tels impacts[47], ce n'est cependant que de manière indirecte, sans que ce soit son objectif premier.

Les limites de l'effectivité du droit

Un autre type de limites de l'encadrement des algorithmes et de l'IA identifiable dans les dispositions juridiques évoquées a trait à l'effectivité même de ces dernières et des principes qu'elles ont vocation à mettre en œuvre. Dans un univers numérique caractérisé par une fluidité et une omniprésence des capteurs rendant difficile l'exercice des droits ainsi que par une forte asymétrie entre ceux qui contrôlent algorithmes et données et les personnes, ces dernières rencontrent des difficultés à exercer leurs droits (par exemple, le droit d'obtenir une intervention humaine dans le cadre d'une décision prise sur le fondement d'un traitement algorithmique, ou encore le droit d'obtenir une information sur la logique sous-tendant le fonctionnement de l'algorithme).

La prise en compte de cette réalité s'est traduite par une série de réflexions récentes, dont certaines se sont traduites dans de nouvelles dispositions légales. Le Règlement européen sur la protection des données à caractère personnel (entrée en application en mai 2018) apporte plusieurs réponses à cette question de l'effectivité du droit dans l'univers numérique, y compris en ce qui concerne les algorithmes[48]. Par ailleurs, la loi pour une République numérique (adoptée en octobre 2016) s'est inscrite dans cette même perspective de renforcement de l'effectivité de principes préexistants.
D'une part, elle a renforcé l'obligation faite à ceux qui déploient des algorithmes d'en informer les personnes concernées. D'autre part, elle prévoit que les codes sources des algorithmes utilisés par l'administration sont des documents communicables, approfondissant ainsi (à l'exception notable du secteur privé) le droit d'obtenir des informations sur la logique mise en œuvre par un algorithme présent dans la loi de 1978.

47 La loi Informatique et libertés limite conditionne notamment au consentement des personnes l'enrichissement de profils individuels par des données collectées sur les réseaux sociaux.
48 L'article 14.1a du Règlement européen, par exemple, renforce le droit à l'information, en prévoyant une information claire et intelligible fournie spontanément par le responsable du traitement algorithmique.

Faut-il interdire les algorithmes et l'intelligence artificielle dans certains secteurs ?

La question de savoir s'il faut interdire les algorithmes et l'intelligence artificielle dans certains secteurs ou pour certains usages ne saurait être éludée d'une réflexion sur les enjeux éthiques soulevés par ces technologies. Rand Hindi évoquait ainsi lors de l'événement de lancement du débat organisé à la CNIL le 23 janvier 2017 la question de savoir s'il faudrait refuser d'automatiser certains métiers pour des raisons éthiques.

Le caractère particulièrement sensible d'un certain nombre de secteurs et des décisions qui y sont prises les désigne assez logiquement comme étant ceux où la question de telles interdictions pourrait se poser. Ainsi, le secteur militaire a récemment fait l'objet d'une pétition internationale demandant que soient bannies les armes autonomes. La médecine ou la justice constituent d'autres domaines où la question pourrait être posée. Certes, comme cela a été rappelé, la législation prévoit d'ores et déjà que le diagnostic du médecin ou la décision du juge ne puissent faire l'objet d'une automatisation. Devant le caractère toujours incertain de la frontière entre délégation et aide à la décision, la question d'un rappel solennel de ces principes pourrait être posée.

Certains secteurs à la sensibilité moins immédiatement évidente font également l'objet de demandes d'interdiction. Ainsi, Serge Tisseron a récemment pris position contre le ciblage personnalisé dans le domaine publicitaire et culturel, accusé de « condamner chaque spectateur à tourner en rond dans ce qu'il connaît de ses goûts et ce qu'il ignore de ses a priori » et de contribuer à « réduire les données dont la majorité des humains disposent pour se faire une opinion sur le monde[49] ».

Enfin, l'interdiction appliquée à tel ou tel usage des algorithmes pourrait porter sur les données utilisées, à l'image du moratoire mis en place par les assureurs français dès 1994 sur le recours aux données génétiques, relayé en 2002 par la loi Kouchner. Dans ce même secteur, une limitation du recours aux données ne serait-il pas une solution possible (légale ou mise en place par les acteurs eux-mêmes) pour maintenir le « voile d'ignorance indispensable » à la pérennité de la mutualisation du risque ?

LE REGARD DU CITOYEN

Les participants à la concertation citoyenne organisée par la CNIL à Montpellier le 14 octobre 2017 (voir « L'organisation du débat public sur les enjeux éthiques des algorithmes et de l'intelligence artificielle ») ont identifié un certain nombre d'enjeux éthiques soulevés par les algorithmes et l'intelligence artificielle. Si leur positionnement révèle des inquiétudes et une conscience des risques, leur attitude générale ne traduit guère d'hostilité de principe à ce que des algorithmes et des outils d'intelligence artificielle se déploient dans notre quotidien, *sous réserve que des réponses soient apportées*.

Parmi les avantages mentionnés dans les différents ateliers de la journée de concertation, figurent la personnalisation du diagnostic médical, la fluidification de processus de recrutement qui deviendraient plus neutres, la simplification de la répartition des étudiants par rapport à l'offre de formation (APB) ou encore l'utilité des filtres sur les plateformes en ligne pour gérer « la multitude d'informations ».

Beaucoup voient positivement les capacités nouvelles d'analyse des données : 63% considèrent ainsi utile de « partager les données pour le bien commun ».

La montée en compétence des participants au cours de la journée de concertation se traduit par un certain accroissement de la conscience des risques : 32% des participants les considéraient comme « plutôt source d'erreur » à l'issue de la journée alors qu'ils n'étaient que 23% ex-ante. Une évolution certes modérée à l'issue d'une journée consacrée aux enjeux éthiques mais qui s'accompagne aussi d'une forme de scepticisme quant à la possibilité d'un encadrement effectif des algorithmes : « est-ce que la loi sera suffisante pour tout contrôler ? Ne sera-t-on pas toujours dans la correction après dérive ? ».

49 http://www.huffingtonpost.fr/serge-tisseron/les-publicites-ciblees-cest-la-betise-assuree-interdisons-les_a_23220999/

Deux principes fondateurs pour le développement des algorithmes et de l'intelligence artificielle : loyauté et vigilance

La réflexion sur les enjeux éthiques soulevés par les algorithmes et l'IA a pour horizon deux dimensions distinctes mais articulées : les principes et les moyens concrets de rendre ceux-ci effectifs.

Le législateur avait inscrit à l'article 1 de la loi Informatique et Libertés que « l'informatique doit être au service de chaque citoyen ». Il s'agit aujourd'hui d'établir les principes permettant d'atteindre cet objectif général et de garantir que l'intelligence artificielle soit au service de l'homme, qu'elle l'augmente plutôt que de prétendre le supplanter.

Les principes inscrits dans la loi Informatique et Libertés et que l'on a rappelés précédemment correspondent-ils toujours aux enjeux qui ont été identifiés et à cet objectif général ? Faut-il en promouvoir de nouveaux ? Outre le constat que ces principes ne couvrent pas la totalité du champ des algorithmes et de l'IA, la circulation dans le débat public d'une série de notions représentant autant d'exigences à l'égard des algorithmes (loyauté, redevabilité, intelligibilité, explicabilité, transparence, etc.) signale à l'évidence le sentiment d'une inadéquation, voire d'inquiétudes.

Au terme du débat public, sont ici présentés une série de principes. Parmi ces derniers, deux en particulier, celui de loyauté et celui de vigilance, apparaissent comme tout particulièrement fondateurs.

Le principe de loyauté

Un principe formulé par le Conseil d'État

Dans son étude annuelle de 2014 sur le numérique et les droits fondamentaux, le Conseil d'État a ainsi formulé trois recommandations invitant à « repenser les principes fondant la protection des droits fondamentaux ». Parmi celles-ci, la première portait sur un principe d' « autodétermination informationnelle » garantissant la maîtrise de l'individu sur la communication et l'utilisation de ses données personnelles et depuis introduit dans la loi pour une République numérique. La troisième portait, elle, sur le principe de « loyauté », appliqué non pas à tous les algorithmes mais, de manière plus restreinte, aux « plateformes[50] ». Selon le Conseil d'État, « la loyauté consiste à assurer de bonne foi le service de classement ou de référencement, sans chercher à l'altérer ou à le détourner à des fins étrangères à l'intérêt des utilisateurs[51] ».

Parmi les obligations des plateformes envers leurs utilisateurs découlant du principe de loyauté tel que défini par le Conseil d'État figurent notamment, d'une part, la pertinence des critères de classement et de référencement mis en œuvre par la plateforme au regard de l'objectif de meilleur service rendu à l'utilisateur et, d'autre part, l'information sur les critères de classement et de référencement mis en œuvre. La première obligation pose donc une limite à la liberté d'établissement des critères de l'algorithme par la plateforme. La deuxième obligation fait de l'information sur la logique de fonctionnement de l'algorithme une obligation incombant à la plateforme (ce n'est pas seulement un droit que l'utilisateur peut choisir ou non de mobiliser).

Avec la loyauté ainsi définie, on accorde par ailleurs moins un droit aux utilisateurs qu'on impose une obligation à l'égard des responsables de traitement.

D'une certaine façon, le principe de loyauté se trouve sous une forme embryonnaire dans la loi Informatique et Libertés de 1978. En effet, le droit à l'information qui s'y trouve affirmé apparaît comme une exigence première de loyauté à l'égard de la personne concernée quant au fait même qu'un algorithme traite ses données. À cela s'ajoute le droit pour toute personne d'interroger le responsable du fonctionnement de l'algorithme pour obtenir des informations quant à la logique suivie par celui-ci ainsi que l'obligation de recueillir le consentement de la personne dont les données sont traitées. L'affirmation même de ces droits dans la loi de 1978 suppose que ces informations soient fournies de manière « loyale » et que le comportement de l'algorithme y corresponde effectivement.

L'intérêt du principe de loyauté tel qu'il est envisagé par le Conseil d'État réside dans la notion d' « intérêt des utilisateurs ». En effet, il ne s'agit pas simplement que l'algorithme dise ce qu'il fait et fasse ce qu'il dise : le principe de loyauté limite aussi la liberté que le responsable de l'algorithme a de déterminer les critères de fonctionnement de ce dernier. D'autre part, alors que dans la loi Informatique et Libertés,

50 Il s'agissait de « soumettre [les plateformes] à une obligation de loyauté envers leurs utilisateurs (les non professionnels dans le cadre du droit de la consommation et les professionnels dans le cadre du droit de la concurrence) ». Les plateformes apparaissent comme des acteurs classant un contenu qu'il n'a pas lui-même mis en ligne.
51 *Le Numérique et les droits fondamentaux,* 2014, p.273 et 278-281

l'information est un droit qui peut éventuellement être mobilisé par l'individu auprès du responsable de l'algorithme, avec le principe de loyauté, cette information doit d'emblée être diffusée à destination de la communauté des utilisateurs[52]. Il n'est pas question ici de droit des utilisateurs mais d'obligation des plateformes algorithmiques. Dans cette mesure, la loyauté semble à même de constituer une réponse au problème de l'asymétrie entre les responsables des algorithmes et les utilisateurs.

La notion de loyauté a notamment fait l'objet de réflexions complémentaires menées par le CNNUM. Celui-ci a en effet initié dans son rapport Ambition numérique (2015) une proposition tendant à créer une « agence de notation de la loyauté des algorithmes » appuyée sur un réseau ouvert de contributeurs, et ce dans un double objectif : rendre accessible via un point d'entrée unique toute une série d'informations déjà rassemblées par les différents acteurs ainsi que les outils existants et ouvrir un espace de signalement de pratiques problématiques ou de dysfonctionnements. Cette initiative pourrait, sous une forme ou sous une autre, participer à une meilleure connaissance citoyenne des enjeux, à une meilleure symétrie entre utilisateurs et plateformes algorithmiques, à une meilleure circulation des bonnes pratiques pour les entreprises ainsi qu'à un repérage facilité des pratiques litigieuses par le régulateur.

Un principe à élargir pour prendre en compte les effets collectifs des algorithmes

Toutefois, par rapport à la définition fournie par le Conseil d'État, **on peut estimer souhaitable d'élargir le principe, au-delà des seules plateformes, à tous les algorithmes**[53]. Par exemple, un algorithme d'aide à la décision en matière médicale, ne devrait-il pas faire l'objet d'une interdiction de recourir, ou du moins d'accorder une place excessive, à un critère lié à l'optimisation de l'occupation des lits d'un hôpital ?

Dès lors, le principe de loyauté des algorithmes aurait aussi l'intérêt de concerner des algorithmes ou des enjeux que ne touchent pas la législation sur la protection des données personnelles. Il concernerait en effet aussi les algorithmes ne procédant pas à un profilage de leurs utilisateurs à des fins de personnalisation de leurs résultats (par exemple, il voudrait pour un moteur de recherche qui ne fournirait pas des résultats profilés).

On pourrait enfin considérer l'opportunité de **reprendre la proposition du Conseil d'État en élargissant, ou du moins en précisant la notion d'« intérêt des utilisateurs », de façon à prendre en compte non seulement la dimension commerciale et économique de cet intérêt, mais également sa dimension collective.** Il s'agirait de considérer que les critères de l'algorithme doivent aussi ne pas entrer trop frontalement en opposition avec certains grands intérêts collectifs, liés notamment au troisième enjeu éthique évoqué précédemment. Ces intérêts collectifs peuvent être entendus de deux façons. D'une part, il peut s'agir de l'intérêt de catégories, de segments constitués par la logique même du big data et de l'analyse algorithmique (des groupes ad hoc, constitués par le croisement de certains traits), qui sont susceptibles de faire l'objet de formes de discriminations. Ces catégories font l'objet des réflexions actuelles portant sur la notion de « group privacy[54] ». D'autre part, cet intérêt collectif peut-être pensé comme celui d'une société tout entière. Par exemple, l'exposition à la diversité culturelle ou d'opinions pourrait être considérée comme liée à « l'intérêt des utilisateurs », entendus certes comme consommateurs mais aussi comme citoyens et parties prenantes d'une collectivité (il conviendrait d'ailleurs d'évoquer directement « l'intérêt des utilisateurs et des citoyens »).

> Les critères de l'algorithme doivent ne pas entrer trop frontalement en opposition avec certains grands intérêts collectifs

Le principe de loyauté des algorithmes, s'il constitue à l'évidence une réponse à d'importants enjeux, se heurte avec la montée en puissance des algorithmes de « machine learning » à une sérieuse difficulté. Ces algorithmes, on l'a vu, peuvent se comporter de façon problématique pour les droits des personnes, y compris à l'insu de leurs concepteurs (biais et discriminations cachés liés aux corrélations effectuées par le système). La notion de loyauté des concepteurs d'algorithmes (ce que l'on entend habituellement de fait par le vocable « loyauté des algorithmes ») perd une part de sa portée dès lors que l'algorithme se comporte d'une façon qui reste opaque à ces mêmes concepteurs. Il faudrait pouvoir parler, au sens propre, de loyauté des algorithmes (mais cela a-t-il un sens ?) ou bien s'assurer que l'algorithme ne se comportera pas d'une façon non souhaitable, sans que l'on soit bien en mesure de préciser a priori ce que l'on entend par ce « non souhaitable ». Autrement dit, **un algorithme loyal ne devrait pas avoir pour effet de susciter, de reproduire ou de renforcer quelque discrimination que ce soit, fût-ce à l'insu de ses**

52 « Sans méconnaître le secret industriel, les plateformes devraient expliquer à leurs utilisateurs la logique générale de leurs algorithmes et, le cas échéant, la manière dont les utilisateurs peuvent les paramétrer. »

53 Précisons – pour couper court à toute inutile querelle sémantique – que l'emploi de l'expression de « loyauté des algorithmes » ne revient pas à anthropomorphiser un fait technique (l'algorithme) mais est un raccourci pratique pour désigner la loyauté de ceux qui conçoivent et déploient l'algorithme.

54 Brent Mittelstadt, From individual to group privacy in Big Data analytics, B. Philos. Technol. (2017) 30: 475. https://doi.org/10.1007/s13347-017-0253-7

concepteurs. Cette dernière piste est donc plus large que les premières réflexions évoquées plus haut sur la notion de loyauté, développées avant tout en référence à des préoccupations d'ordre commerciales, concurrentielles, dans la perspective du développement de pratiques résolument déloyales destinées à obtenir un avantage en manipulant l'algorithme.

Le principe de vigilance

Si le principe de loyauté apparaît comme un principe substantiel fondateur, le principe de vigilance constitue quant à lui un principe plus méthodologique qui doit orienter la façon dont nos sociétés modèlent les systèmes algorithmiques.

L'un des défis identifiés consiste dans **le caractère mouvant et évolutif des algorithmes à l'heure du *machine learning***. Cette caractéristique est renforcée par **l'échelle inédite de l'impact potentiel des algorithmes** exécutés par des programmes informatiques et donc de l'application d'un même modèle. Ceci accroît l'imprévisibilité, le caractère évolutif et potentiellement surprenant des algorithmes et de leurs effets. **Comment donc appréhender et encadrer un objet instable**, susceptible de générer des effets nouveaux au fur et à mesure de son déploiement et de son apprentissage, des effets imprévisibles au départ ?

La promotion d'un principe d'« obligation de vigilance » pourrait être une façon d'aborder ce défi en prévoyant la prise en compte par les concepteurs et ceux qui déploient l'intelligence artificielle de cette caractéristique inédite. Par ailleurs, ce principe d'obligation de vigilance viserait aussi à contrebalancer le phénomène de confiance excessive et de déresponsabilisation dont on a vu qu'il était favorisé par le caractère de boîte noire des algorithmes et de l'IA.

Enfin, **ce principe de vigilance doit avoir une signification collective.** Plus que d'algorithmes, sans doute faudrait-il parler de systèmes algorithmiques, de complexes et longues « chaînes algorithmiques » composées de multiples acteurs (du développeur à l'utilisateur final, en passant par la société ayant collecté les données utilisées pour l'apprentissage, le professionnel qui réalise cet apprentissage, par celui qui a acheté une solution de *machine learning* qu'il va ensuite déployer, etc.). Ce phénomène – semblable à celui qui peut se développer le long d'une chaîne de sous-traitance – favorise la dilution du sentiment de responsabilité, voire simplement de la conscience des impacts que peuvent générer ces outils. Par exemple, le data scientist, s'il occupe une position essentielle, en amont de la chaîne algorithmique, ne saurait détenir toutes les clés et ne possède pas nécessairement la vision d'ensemble de l'action collective dont il forme le premier maillon. Le Conseil National des Barreaux, dans le rapport remis à la CNIL, souligne pour sa part que « le sens de l'éthique du lieu de mise en œuvre du programme peut être très différent de celui du concepteur du programme ». En outre, l'informatique porte en elle-même le risque du développement d'une confiance exagérée dans une machine souvent perçue comme infaillible et exempte des biais charriés par l'action et le jugement humains. La commission Tricot, dans les années 1970, soulignait déjà ce risque. Plusieurs des intervenants du débat public l'ont mentionné cette année. Au total, donc, le développement des systèmes algorithmiques va de pair avec une érosion des vigilances individuelles. Or, il ne saurait être question de laisser se développer ce type d'indifférence face aux impacts possibles des algorithmes et de l'intelligence artificielle. Il est nécessaire d'organiser la vigilance collective, aussi bien à l'égard de phénomènes connus dont il s'agit d'éviter l'apparition qu'à l'égard de phénomènes ou d'impacts qui n'ont pas nécessairement pu être envisagés initialement mais dont l'échelle et le caractère évolutif des nouveaux algorithmes rendent la survenue toujours possible.

> Le développement des systèmes algorithmiques va de pair avec une érosion des vigilances individuelles

Des principes d'ingénierie : intelligibilité, responsabilité, intervention humaine

Intelligibilité, transparence, responsabilité

Face à l'opacité des systèmes algorithmiques, **la transparence** est une exigence très souvent affirmée, non sans lien d'ailleurs avec le principe de loyauté. Selon le Conseil national du numérique, « ce principe implique premièrement et d'une manière générale la transparence du comportement de la plateforme, condition pour s'assurer de la conformité entre la promesse affichée du service et les pratiques réelles. Dans les relations entre professionnels, il s'applique aux conditions économiques d'accès aux plateformes et aux conditions d'ouverture des services à des tiers[55] ». L'opacité en question concerne autant la collecte que le traitement des données par ces systèmes et donc le rôle que ceux-ci jouent dans un certain nombre de prises de décisions. Les algorithmes ne sont pourtant pas opaques seulement à l'égard de leurs utilisateurs finaux ou à ceux dont ils traitent les données. De plus en plus, avec l'affirmation du *machine learning,* les concepteurs mêmes de ces algorithmes probabilistes perdent la capacité à comprendre la logique des résultats produits. C'est donc à un double niveau que se pose la question de l'opacité. La transparence exigée face à cette situation appelle des réponses légales et de procédure mais elle soulève aussi un enjeu technique.

L'idée de transparence des algorithmes est considérée par beaucoup comme excessivement simplificatrice et finalement insatisfaisante : une transparence assimilée à la publication pure et simple d'un code source laisserait l'immense majorité du public, non spécialisé, dans l'incompréhension de la logique à l'œuvre. Par ailleurs, du moins en ce qui concerne le secteur privé, l'idée de transparence entre en tension avec le droit de la propriété intellectuelle, les algorithmes s'apparentant à un secret industriel dont la divulgation pourrait mettre en danger un modèle économique.

Enfin, des entreprises peuvent avancer de bonnes raisons de ne pas dévoiler le code source, ni les critères commandant le fonctionnement d'un algorithme. Ainsi Google cherche-t-il à éviter que les résultats fournis par l'algorithme de son moteur de recherche, PageRank, ne soient faussés par des acteurs qui seraient à même d'en exploiter la logique à leur profit.

De nombreux spécialistes proposent ainsi de préférer, à la transparence, l'exigence **d'intelligibilité** ou d'explicabilité des algorithmes. Plus que d'avoir accès directement au code source, l'essentiel serait d'être à même de comprendre la logique générale de fonctionnement de l'algorithme. Cette logique devrait pouvoir être comprise par tous et donc énoncée verbalement et non sous la forme de lignes de code. C'est ainsi la position de Daniel Le Métayer, de l'Institut national de recherche en informatique et en automatique (INRIA), pour qui l'intelligibilité passe à travers le questionnement sur la logique globale de l'algorithme ainsi que sur des résultats particuliers. C'est la position de Dominique Cardon : « Que doit-on rendre transparent dans l'algorithme ? Est-ce la technique statistique employée ? Faut-il rendre le code visible? Même si c'est utile, il y a des raisons pour qu'il ne soit pas obligatoirement dévoilé. Par exemple, dans le marché du « search engine optimization », des acteurs cherchent à influer sur les résultats de l'algorithme : cela permet de comprendre l'une des raisons pour lesquelles Google ne rend pas son code public. Rendre transparent un calculateur, cela doit avant tout être un travail pédagogique, pour essayer de faire comprendre ce qu'il fait. Ce qui est essentiel, ce n'est pas que le code soit transparent, c'est que l'on comprenne ce qui rentre et ce qui sort de l'algorithme ainsi que son objectif. C'est cela qui doit être transparent » (CNIL, événement de lancement du débat public, 23 janvier 2017).

L'idée d'intelligibilité (ou explicabilité), comme celle de transparence, s'articule de toute façon avec le principe de loyauté, dont on peut considérer qu'elle est finalement une condition de déploiement.

Enfin, l'introduction d'une obligation de redevabilité ou d'organisation de la responsabilité pourrait constituer une réponse au phénomène de dilution de la responsabilité qu'ont tendance à favoriser les algorithmes et l'intelligence artificielle. Il s'agirait de prévoir que le déploiement d'un système algorithmique doit nécessairement donner lieu à une attribution explicite des responsabilités impliquées par son fonctionnement.

55 https://cnnumerique.fr/wp-content/uploads/2015/11/CNNum_Fiche_Loyaute-des-plateformes.pdf

Repenser l'obligation d'intervention humaine dans la prise de décision algorithmique ?

On a vu que la loi de 1978 avait posé un principe d'interdiction de toute prise de décision entraînant des effets juridiques à l'égard d'une personne sur le seul fondement d'un traitement automatisé de données à caractère personnel (autrement dit : sur le seul fondement du résultat fourni par un algorithme analysant des données personnelles). Ce principe est repris dans le Règlement européen sur la protection des données à caractère personnel. Néanmoins, l'un et l'autre de ces textes, immédiatement après avoir affirmé ce principe, le vident en grande partie de sa substance par l'adjonction d'exceptions très larges[56].

Il semble par ailleurs que le recours des juridictions à l'article 10 de la loi de 1978 (dont il est ici question) soit devenu moins fréquent et que l'interprétation dudit article soit devenue moins stricte au cours des quarante dernières années[57]. Une évolution de la Loi Informatique et Libertés intervenue en 2004 a d'ailleurs facilité de fait la prise de décision automatisée, dans le secteur bancaire (credit scoring) par exemple : si l'intervention humaine dans le processus est toujours requise, celle-ci prend la forme d'un droit pour la personne concernée de demander à ce que, en cas de décision défavorable, celle-ci soit réexaminée par une personne. Intervention humaine, donc, mais a posteriori et seulement sur demande.

Sans que le terme implique un jugement de valeur, **il semble que l'on puisse parler d'une forme de « dérive » ou d'évolution du seuil de tolérance de la société à l'égard de la prise de décisions automatisée depuis les années 1970.** L'évolution du droit et de la jurisprudence seraient le reflet de cette évolution. Ne faut-il pas dès lors revisiter le principe interdisant la prise de décision par une machine seule et impliquant donc la nécessaire intervention humaine ? Le revisiter pour accueillir les nouveaux usages de l'IA, sans toutefois y renoncer ?

Dans son étude annuelle de 2014, le Conseil d'État soulignait la nécessité d'assurer l'effectivité de l'intervention humaine. Il est possible de considérer qu'assurer l'effectivité de l'intervention humaine à l'échelle de chaque décision prise revient de fait à empêcher ou à limiter certaines applications des algorithmes et de l'IA. En effet, quand l'automatisation a pour fonction d'optimiser et d'accélérer un processus en remplaçant l'homme, une intervention humaine réellement effective pour chaque décision risque d'être dissuasive. On pourrait en fait poser ainsi la question : comment faire assurer par des machines des tâches auparavant accomplies par l'intelligence humaine (c'est la définition de l'IA) sans évacuer l'homme ? Une façon d'y répondre consiste à avancer que l'on pourrait envisager l'effectivité de l'intervention humaine autrement qu'à l'échelle de chaque décision individuelle. On pourrait, par exemple, assurer que des formes de délibération humaine et contradictoire encadrent et accompagnent l'utilisation des algorithmes en examinant et en interrogeant le paramétrage mais aussi tous les effets – directs et indirects – du système. Cette supervision pourrait ainsi porter, non pas sur chaque décision individuelle, mais de loin en loin sur des séries plus ou moins nombreuses de décisions.

La protection des libertés serait dès lors pensée moins en termes individuels que collectifs. On voit d'ailleurs ici comment une telle piste s'articulerait aussi avec l'idée d'une obligation de vigilance évoquée précédemment. Ce passage d'une interprétation individuelle à une interprétation collective de l'obligation d'assurer une forme d'intervention humaine dans la décision automatisée pourrait faire l'objet d'une modulation en fonction de la sensibilité des applications considérées et de la configuration de la balance avantages/risques (par exemple, dans la santé, faut-il considérer que la sensibilité des enjeux dépasse les gains et justifie donc un maintien de l'obligation de garantir une intervention humaine pour chaque décision ?).

> Comment faire assurer par des machines des tâches auparavant accomplies par l'intelligence humaine (c'est la définition de l'IA) sans évacuer l'homme ?

56 Sur ce point dans le RGPD, voir par exemple : Wachter, Sandra, Brent Mittelstadt, et Luciano Floridi. « Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation ». Social Science Research Network, décembre 2016

57 Voir par exemple la délibération de la CNIL sur le projet GAMIN, en 1981 : la Commission rejeta alors ce projet du ministère de la santé. Même les garanties pourtant données par le ministère pour assurer une intervention humaine effective dans la détection de mineurs à risques psycho-sociaux dont il était question furent repoussées. On peut pourtant se demander à la lecture du dossier si la position de la CNIL serait aujourd'hui la même, alors qu'il nous semble qu'une certaine accoutumance s'est opérée à l'idée de voir des algorithmes intervenir de plus en plus fortement dans des domaines de plus en plus importants. Par exemple, la décision d'éliminer des candidats sur le fondement d'un seul traitement automatisé ne paraît guère relever de la science-fiction ni même probablement de ce que beaucoup dans notre société sont prêts à accepter.

Des principes aux recommandations pratiques

Comment donner une effectivité concrète aux principes abordés précédemment ? Les pages suivantes listent les principales recommandations qui ont émergé du débat public organisé par la CNIL de janvier à octobre 2017, complété par la consultation de rapports déjà émis par diverses institutions en France et à l'étranger (entre autres, l'OPECST, la CERNA, le CNNUM, le Conseil d'État, la CGE, la Maison Blanche, France IA, INRIA, AI Now).

Une idée générale qui émane de la plupart des réflexions est que les solutions impliquent nécessairement une palette d'actions diversifiées concernant différents acteurs (les concepteurs d'algorithmes, les professionnels, les entreprises, la puissance publique, la société civile, l'utilisateur final). Les systèmes algorithmiques et d'intelligence artificielle sont des objets socio-techniques complexes, modelés et manipulés par de longues et complexes chaînes d'acteurs. **C'est donc tout au long de la chaîne algorithmique** (du concepteur à l'utilisateur final, en passant par ceux qui entraînent les systèmes et par ceux qui les déploient) **qu'il faut agir, au moyen d'une combinaison d'approches techniques et organisationnelles.** Les algorithmes sont partout : ils sont donc l'affaire de tous.

La loi ne saurait être le seul levier, la solution passant nécessairement par une mobilisation de tous les acteurs. Un certain nombre des recommandations formulées ci-dessous ne précisent d'ailleurs pas si c'est la loi ou l'initiative spontanée des différents acteurs qui devrait être privilégiée pour les mettre en œuvre.

LE REGARD DU CITOYEN

Les participants à la concertation citoyenne organisée par la CNIL à Montpellier le 14 octobre 2017 (voir « L'organisation du débat public sur les enjeux éthiques des algorithmes et de l'intelligence artificielle ») ont formulé des recommandations. Ces dernières recoupent en grande partie celles recueillies ailleurs dans le cadre du débat public.

- Le souhait que l'humain garde le contrôle sur le développement des algorithmes apparaît prioritaire (95% d'avis favorables), une délégation excessive des décisions aux algorithmes et à l'IA étant jugée préjudiciable. Le constat des participants rejoint l'idée d'un principe de vigilance précédemment évoqué : 97% souhaitent « garder la dimension humaine, garder une dose de subjectivité, ne pas de désinvestir totalement » et 91% considèrent que « l'utilisateur devrait être dans une posture d'apprenant à chaque usage d'un algorithme afin d'en cerner les limites et être exigeant vis-à-vis des développeurs à chaque fois que cela est nécessaire ». Dans le champ de la médecine par exemple, certains citoyens pensent qu'une partie des décisions devrait toujours être discutée en collège.

- L'adaptation de la formation des concepteurs d'algorithmes est une option ayant émergé dans plusieurs groupes de travail, et ayant fait l'objet d'un quasi-consensus : 97% des participants considèrent que « les développeurs doivent intégrer dans leurs pratiques une certaine éthique et résister aux demandes tentantes du marché qui peuvent affecter cette dimension ». 94% en appellent ainsi au développement de chartes éthiques et 56% souhaiteraient que des experts associés issus des sciences humaines et sociales permettent aux développeurs de mieux mesurer l'impact de leur travail sur la société. La formation concerne également les utilisateurs d'algorithmes : 82% des personnes présentes sont favorables à une obligation de formation continue des médecins utilisant des systèmes d'aide à la décision. Plus généralement, ce besoin de savoir et de comprendre se matérialise par une forte demande pour plus d'éducation au numérique tout au long de la vie. Notamment afin de lutter contre les inégalités face à ces objets, l'intégralité des citoyens revendiquent une « éducation populaire au numérique » et le « développement de programmes scolaires pour une « alphabétisation » au numérique tant sur l'objet que sur les enjeux ».

LE REGARD DU CITOYEN (suite)

- La nécessité de disposer de droits renforcés en matière d'information, de transparence et d'explication quant à la logique de fonctionnement de l'algorithme a également été vigoureusement affirmée dans chacun des groupes de travail. C'est déjà la possibilité d'être informé dès qu'un algorithme est déployé qui semble être exigée par les participants : 88% des participants estiment en effet qu'un employeur qui utilise un algorithme devrait impérativement l'indiquer aux candidats. La mise à disposition des codes source est jugée souhaitable par 78% d'entre eux, bien qu'elle soit considérée comme insuffisante pour comprendre les résultats produits par un algorithme. Dans le cas d'APB par exemple, un accompagnement plus effectif pour comprendre les ressorts de son utilisation est demandé par 78% des citoyens présents. 85% voient d'ailleurs dans l'expérience des utilisateurs un matériau précieux pour « améliorer l'ergonomie de la procédure ». Lorsqu'un critère de l'algorithme repose sur des choix politiques (le tirage au sort, par exemple), il convient également de ne pas l'occulter mais bien au contraire de le rendre lisible (selon 94% des participants). Notons que si un désir de transparence se manifeste, il n'est pas unanime et s'accompagne d'une lucidité voire d'un fatalisme sur l'hypothèse qu'elle puisse suffire.

- Un effort étatique de régulation pour identifier les biais, « éviter les abus, établir des statistiques et imposer un agrément » pourrait constituer une solution selon une écrasante majorité des participants (97%). Beaucoup préconisent la création d'un organisme indépendant pour effectuer des tests scientifiques sur les algorithmes, « à l'image des médicaments avant la mise en vente sur le marché » (84%). Sur le long terme, s'assurer régulièrement que l'algorithme soit « toujours en phase avec les objectifs visés » constitue également une idée ayant émergé des débats (63% y sont favorables). L'intervention du législateur est également vivement souhaitée (94%) afin de mieux intégrer l'éthique dans les lois « à travers des chartes et des règles déontologiques, des formations, des concertations ».

- L'importance pour la société civile de s'organiser face à ces objets technologiques nouveaux a aussi été avancée par certains des participants à travers notamment le rôle du tissu associatif (associations de patients dans le champ de la santé), la protection nécessaire des lanceurs d'alerte, ou encore le soutien apporté à des réseaux alternatifs aux plateformes du web dont les algorithmes utilisés poseraient question.

- Enfin, les échanges ont démontré un fort attachement à la protection des données à caractère personnel et à la protection de la vie privée. La question de savoir à qui appartiennent nos données et quels sont les usages qui en sont faits a été jugée prioritaire dans certains groupes de travail, sur la santé notamment, ou encore sur l'emploi (inquiétude sur la possibilité que des algorithmes analysent des données qui seraient collectées en dehors de l'entreprise).

RECOMMANDATION 1

Former à l'éthique tous les maillons de la « chaîne algorithmique » : concepteurs, professionnels, citoyens

Formation des citoyens

Le citoyen est l'un des acteurs centraux des systèmes algorithmiques. D'une part car les algorithmes ont un impact croissant sur son existence. D'autre part, parce qu'il est particulièrement bien placé pour en identifier les éventuels dérives. Lui fournir les clés de compréhension lui permettant d'aborder de manière confiante, active et éclairée ces nouvelles technologies est une nécessité qui correspond par ailleurs à une demande de sa part, ainsi que l'a rappelé fortement la concertation citoyenne organisée à Montpellier par la CNIL le 14 octobre 2017.

L'impératif de constituer une « nouvelle littératie » numérique à intégrer dès l'école et jusqu'à l'université fait l'objet d'un large consensus. Des acteurs comme le CNNUM ont déjà développé des réflexions à cet égard[58]. Cette littératie numérique comprendrait évidemment une culture algorithmique dont les fondements peuvent d'ailleurs être posés très tôt, par des exercices qui n'impliquent pas nécessairement le recours à un matériel numérique.

58 https://cnnumerique.fr/education-2/

La diffusion de cette culture algorithmique très largement dans la population peut être également favorisée par l'encouragement aux initiatives de médiation numérique dans les territoires. Autrement dit, une forme d'éducation populaire numérique incluant une dimension d'appropriation aux données et aux algorithmes. Citons par exemple les initiatives de la FING (Info Lab), de la Péniche à Grenoble (Coop-Infolab), de Pop School à Lille.

Formation des concepteurs d'algorithmes

Les concepteurs d'algorithmes (développeurs, programmeurs, codeurs, data scientists, ingénieurs) forment le premier maillon de la chaîne algorithmique. Ils occupent à ce titre une position particulièrement sensible. La technicité de leurs métiers est par ailleurs susceptible de rendre leurs actions opaques (et donc difficilement contrôlables) aux autres acteurs. Il est capital qu'ils aient une conscience aussi claire que possible des implications éthiques et sociales de leurs actions, et du fait même que ces dernières peuvent recouvrir la dimension de choix de société qu'ils ne sauraient être légitimes à arbitrer seuls. Or, **l'organisation concrète du travail et de l'économie tend à segmenter les tâches et à favoriser la tendance que peuvent avoir les individus à ignorer les implications de leur activité au-delà de leur silo.** Par conséquent, il est nécessaire que leur formation même mette les concepteurs des algorithmes en capacité de saisir ces implications parfois très indirectes sur les personnes mais aussi sur la société, qu'elle les responsabilise en éveillant leur *vigilance*.

L'intégration, dans la formation des ingénieurs et data scientists, de l'approche des sciences humaines et sociales (sociologie, anthropologie, gestion, histoire des sciences et des techniques, sciences de l'information et de la communication, philosophie, éthique) sur ces questions peut à cet égard avoir des effets positifs.

Le développement de ces mêmes enseignements bénéficierait de l'intégration des approches techniques et des sciences humaines et sociales au sein de laboratoires interdisciplinaires.
Certaines initiatives vont déjà dans ce sens. Citons par exemple le cas de l'ENSC (École nationale supérieure de cognitique, à Bordeaux), grande école intégrant les sciences humaines et sociales au cursus de formation de ses ingénieurs ou encore le laboratoire Costech (Connaissance, organisation et systèmes techniques), à l'Université Technique de Compiègne (UTC).

Enfin, il est essentiel de favoriser la diversification culturelle, sociale et de genre des professions impliquées dans la conception des algorithmes afin de garantir que l'intelligence artificielle ne favorise pas des formes d'ethnocentrisme. La féminisation de ces métiers devrait notamment commencer par un effort d'ouverture des filières de formation aux femmes.

Formation des professionnels utilisateurs d'algorithmes

Pour considérer l'ensemble de la chaîne de déploiement des algorithmes, il est nécessaire d'envisager également la formation des professionnels appelés à utiliser ces systèmes dans le cadre de leur activité. Il s'agirait notamment de les armer contre le risque de déresponsabilisation, de perte d'autonomie que peut développer le recours à des outils fonctionnant parfois comme des boîtes noires présentées comme étant d'une efficacité imparable. Prévenir le développement d'une confiance excessive en sensibilisant aux dimensions éthiques d'une prise de décision qui ne doit pas exclure l'intervention humaine et en développant l'esprit critique s'avère crucial dans des secteurs particulièrement sensibles, comme peuvent l'être la médecine, le recrutement, la justice, et peut-être dès maintenant surtout le marketing, où les catégories antisémites récemment générées par les algorithmes apprenants de Facebook sont venus illustrer la réalité des risques. Cette formation devrait notamment inclure, dans une optique pluridisciplinaire, la prise en compte des enjeux spécifiques que posent ces outils à chaque secteur. Un médecin qui utilise un système d'aide au diagnostic recourant à l'intelligence artificielle, par exemple, devrait être rendu spécifiquement attentif au développement possible de biais et capable d'une réflexivité à la hauteur de l'outil qu'il maniera et des conséquences de ses erreurs.
On pourrait ainsi imaginer la création de sorte de « permis d'utiliser les algorithmes et l'IA » dans certains secteurs, acquis grâce à des modules de formations spécifiques que délivreraient universités et écoles spécialisées.

Sensibilisation des acteurs publics à la nécessité d'un usage équilibré et « symétrique » des algorithmes

De même, il serait souhaitable de sensibiliser les acteurs publics à la nécessité d'un déploiement équilibré et symétrique des algorithmes. Alors que ces derniers sont de plus en plus utilisés pour lutter la fraude et à des fins de contrôle, laisser se développer dans le public la perception erronée selon laquelle ils ne peuvent servir qu'au contrôle et à des finalités répressives (par ailleurs utiles aux individus mêmes) risquerait de générer une forme de défiance qui serait à terme néfaste à leur déploiement et à l'exploitation de leurs avantages. Il serait donc hautement souhaitable que les responsables administratifs et politiques soient convaincus de l'utilité d'exploiter les potentialités des algorithmes qui apparaissent immédiatement favorables aux personnes et permettent d'améliorer l'accès aux droits (détection du non-recours aux aides sociales)[59].

59 Dans une évaluation des politiques publiques en faveur de l'accès aux droits sociaux, les députés Gisèle Biémouret et M. Jean-Louis Costes proposaient en 2016 de « mettre les outils de lutte contre la fraude au service de la diminution du non recours aux droits sociaux ». Voir : Rapport d'information du comité d'évaluation et de contrôle des politiques publiques sur l'évaluation des politiques publiques en faveur de l'accès aux droits sociaux.

RECOMMANDATION 2

Rendre les systèmes algorithmiques compréhensibles en renforçant les droits existants et en organisant la médiation avec les utilisateurs

L'opacité, pour les personnes, des algorithmes qui les profilent et de la logique à laquelle ceux-ci obéissent, pour leur attribuer un crédit bancaire par exemple, n'est pas sans trouver de premiers éléments de réponse dans le droit existant. De même, on a vu que celui-ci contient depuis longtemps des dispositions ouvrant la voie à une première forme d'intelligibilité et de transparence[60].

En revanche, de nombreux diagnostics convergent pour souligner l'insuffisance de ces dispositions pour résorber de manière effective l'opacité des systèmes algorithmiques et assurer intelligibilité, transparence et loyauté. Instaurer pour les responsables des systèmes une obligation de communication (et non pas sur la seule demande formulée par les personnes concernées) claire et compréhensible des informations permettant de comprendre la logique de fonctionnement d'un algorithme serait une façon de répondre à cet enjeu. Elle a d'ailleurs été d'ores et déjà prévue dans la loi pour une République numérique pour les algorithmes déployés par les administrations publiques[61].

On peut également considérer qu'il serait souhaitable que cet impératif (qu'il soit fixé par la loi ou librement adopté par les acteurs) concerne aussi les algorithmes n'impliquant pas le traitement des données personnelles de leurs utilisateurs, dans la mesure où ceux-ci sont susceptibles d'avoir des impacts collectifs significatifs, même si ceux-ci ne portent pas directement sur des personnes (voir notamment « Les limites de l'encadrement juridique actuel des algorithmes » et « Le principe de loyauté »).

Une telle obligation, inscrite dans la loi, pourrait opportunément être prolongée par des initiatives privées enclenchant une dynamique vertueuse. Pour les acteurs du web ayant des sites sur lesquels les personnes disposent d'un compte auquel elles peuvent se connecter, l'information sur leur « profil », les données traitées et inférées et la logique de l'algorithme pourraient être accessibles dans cet espace. Les personnes pourraient par ce biais corriger et actualiser aisément leur profil et les données les concernant.

Cette évolution du droit pourrait être relayée par le développement de bonnes pratiques par les acteurs, à l'aide d'outils de droit souple.

Le problème de l'opacité des algorithmes tient aussi au fait que **les responsables des systèmes algorithmiques ne sont pas, dans l'immense majorité des cas, concrètement joignables ou accessibles pour fournir ces informations et explications.** Ceci implique également une irresponsabilité de systèmes auxquels les utilisateurs se trouvent dans l'impossibilité de demander des comptes. **Il est donc nécessaire d'organiser une forme de « joignabilité » des systèmes algorithmiques,** notamment en identifiant systématiquement au sein de chaque entreprise ou administration une équipe responsable du fonctionnement d'un algorithme dès lors que celui-ci traite les données de personnes physiques. Il est en outre nécessaire de communiquer délibérément et de façon claire l'identité et les coordonnées de cette personne ou de cette équipe de façon à ce qu'elle puisse être contactée aisément et qu'elle ait les moyens de répondre rapidement aux demandes reçues.

La joignabilité devrait être aussi accompagnée d'un effort résolu pour organiser la médiation et le dialogue entre les systèmes et la société, conformément aux idées développées par la Fondation Internet Nouvelle Génération (FING) dans le cadre de l'initiative « NosSystèmes ». La FING constate en effet que « joindre le responsable technique ne suffit pas ». Elle propose ainsi, par exemple, la mise en place d'équipes dédiées à la qualité du dialogue usager ainsi que d'un « pourcentage médiation ». Alors que les algorithmes permettent des économies d'échelle, prendre en compte le pourcentage du budget d'un projet consacré à l'effort de médiation (mise en place d'outils de visualisation, équipe de médiation, partenariat, contrôle de la bonne compréhension de l'information, etc.) pourrait permettre – via des procédures de certification – de valoriser et de conférer un avantage concurrentiel (en termes d'image aux yeux des consommateurs) aux systèmes vertueux.

RECOMMANDATION 3

Travailler le design des systèmes algorithmiques au service de la liberté humaine

Plus que l'algorithme seul, voire le programme exécutant l'algorithme, c'est à l'ensemble du système algorithmique qu'il s'agit de s'intéresser pour en comprendre et en contrôler les effets. De nombreuses réflexions récentes mettent en avant l'importance de prendre en compte le design des systèmes algorithmiques, c'est-à-dire l'interface entre la machine et son utilisateur.

60 Notamment l'article 39 de la Loi Informatique et libertés, organisant le droit d'accès.
61 L'article 14.1a du Règlement européen va dans ce sens en prévoyant une telle information.

Il convient ainsi d'agir sur le design pour contrer le caractère de « boîtes noires » que peuvent avoir les algorithmes dès lors qu'ils se présentent comme des systèmes opaques présentant des résultats sans mise en perspective de leurs propres limites ni présentation de la manière dont ils sont construits mais parés du prestige de la neutralité et de l'infaillibilité si facilement prêtées à la machine.

À l'inverse, il s'agit de promouvoir un design propre à renforcer l'autonomie et la réflexivité des personnes, à remédier aux situations d'asymétrie que peuvent établir les algorithmes à leur détriment, à leur permettre de prendre des décisions informées et de manière lucide.

Par exemple, la mise en place de systèmes de visualisation permettant de redonner plus de contrôle à l'utilisateur en lui donnant une meilleure information va dans ce sens. **Des outils de visualisation peuvent permettre à des individus de comprendre pourquoi des recommandations leur ont été proposées voire, encore mieux, de générer en retour des recommandations plus appropriées.** Les individus se trouvent par-là même placés dans une posture active. Il s'agit de donner à l'individu la main sur une partie au moins des critères qui déterminent la réponse fournie par l'algorithme, lui permettant éventuellement de tester différentes réponses en fonction de paramétrages différents. Un exemple d'outil de visualisation a été fourni au cours du débat public par la présentation du « Politoscope[62] ». Développé par l'Institut des Systèmes Complexes de Paris-Île de France, le politoscope permet au grand public de plonger dans des masses de données et de voir l'activité et la stratégie des communautés politiques sur les réseaux sociaux et notamment sur Twitter. Il aide à contrebalancer, en la dévoilant, la pratique de l'astroturfing, c'est-à-dire la manipulation à leur avantage par des groupes très organisés des réseaux sociaux pour imposer certains thèmes à l'ordre du jour de la scène politique nationale. Il participe ainsi à un rééquilibrage dans l'utilisation des algorithmes, dans le but de préserver un accès démocratique à l'information.

À travers le design, c'est toute la relation entre l'homme et la machine qui peut être modifiée, dans le sens d'une responsabilisation de l'homme et d'une augmentation de sa capacité à prendre des décisions éclairées, au lieu d'une confiscation au profit de la machine de sa capacité à faire des choix. C'est en somme au *principe de vigilance* évoqué plus haut qu'il s'agit ici de donner corps.

Le concept de « jouabilité » récemment proposé par la FING dans le cadre de son expédition « NosSystèmes » pourrait également constituer un principe régissant le design de systèmes algorithmiques vertueux, mis au service de l'individu et de sa capacité d'agir dans toute sa plénitude. Il s'agit de permettre aux utilisateurs de « jouer » avec les systèmes en en faisant varier les paramètres. Permettre par exemple aux utilisateurs d'APB de pouvoir le tester « à blanc » en voyant les résultats fournis en fonction de différents choix avant d'entrer leurs vœux définitifs. On pourrait ainsi imaginer également qu'un moteur de recherches sur internet permette à ses utilisateurs de lancer plusieurs recherches en faisant varier les critères. L'idée de jouabilité repose sur le fait que **toucher et manipuler est la clé d'une compréhension directe,** bien davantage sans doute que l'accès à un code source indéchiffrable pour la grande majorité d'entre nous.

> À travers le design, c'est toute la relation entre l'homme et la machine qui peut être modifiée, dans le sens d'une responsabilisation de l'homme et d'une augmentation de sa capacité à prendre des décisions éclairées

RECOMMANDATION 4

Constituer une plateforme nationale d'audit des algorithmes

Développer l'audit des algorithmes de manière à contrôler leur conformité à la loi et leur loyauté est une solution fréquemment évoquée pour assurer leur loyauté, leur responsabilité et, plus largement, leur conformité à la loi.

Développer l'audit des algorithmes signifie d'abord développer la capacité de la puissance publique à assurer ce dernier. L'audit des algorithmes n'est pas une réalité nouvelle. La Commission des sanctions de l'Autorité des marchés financiers s'est ainsi appuyée sur l'analyse de l'algorithme « Soap » pour rendre sa décision du 4 décembre 2015 à

62 https://politoscope.org/

l'égard des sociétés Euronext Paris SA et Virtu Financial Europe Ltd. De même, la CNIL dispose, pour son activité de contrôle, des compétences d'auditeurs des systèmes d'information. L'Autorité de la concurrence doit aussi appuyer de plus en plus son activité sur une capacité à auditer les algorithmes.

Il est donc essentiel que la puissance publique se donne autant que possible les moyens d'ouvrir le code source d'algorithmes déterministes. Or, ces moyens s'avèrent de plus en plus insuffisants face à un besoin croissant. La CNIL se trouve ainsi désormais sollicitée par d'autres régulateurs sectoriels dépourvus de toute capacité d'audit. **Un travail de recensement des ressources de l'État, des différents besoins ainsi qu'une mise en réseau des compétences et des moyens au moyen d'une plateforme nationale est donc aujourd'hui une nécessité.**

Une telle plateforme devrait aussi avoir pour fonction de relever le défi que soulève le développement du *machine learning.* Celui-ci conduit certains à souligner que l'examen des codes sources s'avère peu réaliste dès lors qu'il s'agit d'analyser des millions de lignes de code. Or, auditer ne signifie pas nécessairement ouvrir les codes sources. Cela peut aussi prendre la forme de contrôles ex post des résultats produits par les algorithmes, de tests aux moyens de profils fictifs, etc. Ces techniques d'audit reposant sur la rétro-ingénierie doivent faire l'objet d'un effort de recherche significatif (cf. recommandation suivante).

Opérationnellement, la mise en œuvre de ces audits pourrait être assurée par un corps public d'experts des algorithmes qui contrôleraient et testeraient les algorithmes (en vérifiant par exemple qu'ils n'opèrent pas de discrimination). Une autre solution pourrait consister, notamment face à l'ampleur du secteur à contrôler, à ce que la puissance publique homologue des entreprises d'audit privées sur la base d'un référentiel. Certaines initiatives privées ont d'ailleurs d'ores et déjà vu le jour. Par exemple, Cathy O'Neil, plusieurs fois citée dans ce rapport, a créé la société « Online Risk Consulting & Algorithmic Auditing », une entreprise dont l'objectif est d'aider les entreprises à identifier et à corriger les préjugés des algorithmes qu'elles utilisent.

Indépendamment même d'une obligation de recourir à la procédure d'audit, il est souhaitable que les entreprises et les administrations se tournent vers des solutions de type « label ». Ces labels pourraient alimenter une dynamique vertueuse. D'une part, ils garantiraient la non-discrimination et la loyauté des algorithmes. D'autre part, ils offriraient aussi une visibilité aux efforts en vue de la mise en place d'un design ainsi qu'en vue de la mise en place d'une information proactive et adaptée, conformément aux recommandations précédentes, donc, et au-delà même des strictes obligations légales.

RECOMMANDATION 5

Encourager la recherche de solutions techniques pour faire de la France le leader de l'IA éthique

Favoriser l'explication sur le fonctionnement et la logique des algorithmes.
Fournir aux régulateurs, aux entreprises et aux citoyens des outils robustes pour contrôler, maîtriser et surveiller les impacts des algorithmes et de l'intelligence artificielle, pour en comprendre la logique de fonctionnement devrait constituer un axe croissant des politiques de recherche.

Le développement de **techniques de rétro-ingénierie** pour « tester » le caractère non discriminatoire, la capacité à **pré-traiter les données pour réduire les risques de discrimination** en identifiant et résolvant les biais des jeux d'apprentissage[63], la **génération d'explications en langage naturel par les machines algorithmiques recourant à l'apprentissage automatique des résultats qu'elles produisent** mériteraient de faire l'objet d'un investissement significatif.

En France, le projet TransAlgo, conduit par INRIA, a d'ores et déjà pour objectif de catalyser la dynamique sur ces questions à travers l'élaboration d'une plateforme scientifique. Le projet Algodiv (recommandation algorithmique et diversité des informations du web) vise quant à lui à apporter des réponses aux questions posées par la notion d'enfermement : les algorithmes nuisent-ils à la diversité et à la sérendipité ? Ces projets ont en somme pour but de fournir une meilleure compréhension d'un certain nombre de problèmes évoqués dans le présent rapport.

Des initiatives visant à articuler interdisciplinarité, recherche de pointe et développement d'outils devraient être soutenues en France, à l'instar de celle du Professeur Katharina Anna Zweig en Allemagne qui a créé en 2017 le laboratoire « Algorithmic Accountability Lab ». Ce dernier, outre une activité d'analyse appuyée sur les sciences dures, les sciences techniques et les sciences humaines (conformément à l'idée que les systèmes algorithmiques ne peuvent être compris, prédits et contrôlés que dans le contexte de leur application), vise à développer un design transparent, éthique et responsable des systèmes automatisés d'aide à la décision. Il propose en outre des outils didactiques

63 La construction d'un jeu de données non-biaisées a fait cette année l'objet d'un projet mené par l'association Open Law, partenaire du débat public animé par la CNIL.

concernant les risques et promesses des ADM[64] pour, à la fois, le grand public et les preneurs de décision[65].

Un autre exemple est fourni par la constitution récente aux États-Unis de l'Institut de recherche *AI Now* (au sein de la New York University) dont l'objet est d'examiner les implications sociales de l'intelligence artificielle. L'implication dans cette structure du « Partnership on AI », initiative notamment d'Amazon, Apple, Google, IBM et Microsoft amène toutefois à souligner l'attention toute particulière qui devrait être attachée à la composition de telles institutions. Comme l'a récemment souligné l'ancienne universitaire Cathy O'Neil, l'importance de l'implication du monde de la recherche dans le travail d'élucidation des impacts sociaux de l'IA tient aussi à la valeur toute particulière de la liberté académique[66].

Développer des infrastructures de recherche respectueuses des données personnelles

Le développement d'une IA respectueuse des données constitue un enjeu croissant alors que les citoyens en Europe, mais aussi plus largement dans le monde entier, se montrent de plus en plus soucieux de la protection de leurs données personnelles et aux risques générés. Diverses pistes peuvent ici être évoquées dans la perspective de la construction d'un nouvel équilibre, fondé sur un renforcement symétrique des capacités d'accès des chercheurs à d'importants jeux de données et de la sécurité de ces mêmes données

Tout d'abord **le développement d'espaces sécurisés pour l'accès à des données** à des fins de recherche et d'entraînement des algorithmes d'intelligence artificielle. Par exemple, des travaux comme ceux conduits dans le cadre du projet OPAL, participent de cette dynamique. Ce projet vise à bâtir une infrastructure sur laquelle les données d'opérateurs téléphoniques sont stockées et peuvent être analysées en toute sécurité au moyen d'algorithmes certifiés mis à disposition des utilisateurs et enrichissables par la communauté. Avec de tels systèmes, les données ne sont pas directement accessibles à ceux qui les exploitent, garantissant la protection des personnes. La certification des algorithmes qui peuvent être utilisés pour analyser ces jeux de données a une fonction de filtrage éthique des données, ce qui permet notamment de faire face aux défis posés en termes de « *group privacy*[67] ».

Des bases à la main d'acteurs publics tels que le CASD (Centre d'Accès Sécurisé aux Données) utilisées pour la mise à disposition de bases de données de l'administration à des fins de recherche constituent également une piste à suivre.

Lancer une grande cause nationale participative pour dynamiser la recherche en IA

La capacité à disposer de très vastes quantités de données constitue l'un des fondements du développement d'une recherche en IA. Contrairement à une image trop souvent répandue, les législations française et européenne proposent un cadre suffisamment ouvert pour soutenir une recherche et une politique industrielle ambitieuses en la matière. Au-delà des possibilités évoquées ci-dessus, la création par le Règlement européen de protection des données (RGPD) d'un « droit à la portabilité », qui permet aux personnes de récupérer leurs données conservées par des acteurs privés, ouvre de grandes opportunités encore largement inconnues.

La puissance publique pourrait jouer un rôle moteur dans la concrétisation de ces dernières. Elle pourrait ainsi **lancer une grande cause nationale ou un grand projet de recherche fondé sur des données issues de la contribution de citoyens exerçant leur droit à la portabilité auprès des acteurs privés** et rebasculant leurs données pour un projet au service d'une cause d'intérêt général. L'Etat se porterait garant du respect des libertés par le projet et pourrait, par exemple, soutenir la mise en place d'un tableau de bord (sur le modèle du projet « NosSystèmes » de la FING) à la main des personnes. Au-delà de ce seul projet, la puissance publique amorcerait ainsi les potentialités ouvertes par la création du droit à la portabilité.

Les acteurs privés pourraient naturellement apporter leurs propres jeux de données à ce projet et participer à cette grande cause nationale.

RECOMMANDATION 6

Renforcer la fonction éthique au sein des entreprises

Identifier de possibles irrégularités ou effets néfastes en amont du déploiement d'algorithmes aux impacts significatifs, mais également assurer un rôle de veille en continu pour identifier les problèmes émergents, imperceptibles ou inaperçus au départ, en apportant un contrepoint à la perspective des opérationnels s'avère aujourd'hui une fonction essentielle des entreprises. Il s'agit aussi de développer une vision générale de chaînes algorithmiques dont on a souligné la tendance à la segmentation et à la compartimentation des fonctions et des préoccupations. Du même impératif participe la nécessité d'organiser des formes de dialogue entre opérationnels, personnalités extérieures à

64 Algorithmic Decision Making Systems.

65 Plusieurs projets ont déjà émergé de ce laboratoire, notamment, le projet de « dons-de-données » (en allemand « Datenspende Projekte » https://datenspende.algorithmwatch.org/), dans lequel plus de 4000 utilisateurs ont observé, pendant plusieurs mois avant et jusqu'à l'élection parlementaire allemande, les résultats de recherches Google concernant les 16 principaux candidats. L'idée sous-jacente de ce projet est de mesurer l'impact de la personnalisation par Google des résultats de recherches afin de confirmer ou d'infirmer la théorie appelée « filter bubble ».

66 https://www.nytimes.com/2017/11/14/opinion/academia-tech-algorithms.html

67 Des projets précédents ont montré que l'usage de données anonymisées était susceptible de générer des usages problématiques du point de vue éthique (ciblage de groupes de population – et non pas forcément d'individus – sur une base ethnique dans des contextes de conflit, segmentation actuarielle, etc.).

> Assurer un rôle de veille en continu pour identifier les problèmes émergents, imperceptibles ou inaperçus au départ s'avère aujourd'hui une fonction essentielle des entreprises

l'entreprise, acteurs et communautés impliquées par le fonctionnement des algorithmes ainsi que chercheurs en sciences humaines et sociales.

Plusieurs modalités de mise en œuvre de cet impératif pourraient être envisagées.

Une solution pourrait consister dans le déploiement de comités d'éthique au sein des entreprises déployant des algorithmes aux impacts significatifs. La composition et les modalités d'intervention de tels comités constituent un point essentiel. Publicité ou non des comptes rendus, publicité ou non de la composition du comité, degré éventuel d'indépendance: la palette des options possibles est large.

L'attribution de cet impératif à la fonction RSE ou aux déontologues pourrait également être envisagée.

Cette animation de la fonction de réflexion éthique dans le secteur privé pourrait aussi prendre la forme de réseaux constitués par secteurs ou branches professionnelles pour assurer la diffusion de bonnes pratiques ainsi que le repérage précoce de problèmes émergents. On pourrait d'ailleurs même considérer que des comités éthiques sectoriels puissent organiser une forme de veille éthique en lieu et place de comités installés au niveau de chaque entreprise, ce qui constituerait néanmoins une garantie moindre.

Ce travail en réseau devrait avoir pour objectif la constitution et la tenue à jour de référentiels éthiques sectoriels (chartes éthiques, codes de conduite, chartes de déontologie etc.), mais également la révision des codes d'éthique professionnels préexistants pour prendre en compte l'introduction des algorithmes et des systèmes d'IA.

Ces réflexions devraient en retour déboucher sur l'intégration, dans les chartes de déontologie des entreprises, d'un chapitre dédié aux enjeux soulevés par les algorithmes (en explicitant par exemple les limites à ne pas franchir en concevant les paramètres des systèmes, des obligations de qualité et d'actualisation des jeux de données utilisés pour entraîner les algorithmes, etc.).

Les diverses possibilités évoquées dans les paragraphes précédents ont pour but de souligner que la formule exacte à retenir mériterait sans doute de faire l'objet de débats spécifiques et que, à l'évidence, plusieurs positions peuvent exister.

CONCLUSION

Les principes et les recommandations formulés à l'issue de ce rapport constituent le résultat de la synthèse par la CNIL des échanges et des réflexions menés à l'occasion du débat public national qu'elle a animé, grâce au soutien de soixante partenaires, de janvier à octobre 2017.

Les recommandations ont été formulées de façon très large, mobilisant tout le spectre possible des acteurs publics ou privés. Les défis soulevés par les algorithmes appellent une mobilisation, une attention et un questionnement de la part de l'ensemble des acteurs de la société civile (citoyens, entreprises, associations) pour piloter un monde complexe. Il ne s'agissait donc pas d'avancer que le véhicule à privilégier pour les appliquer ne pouvait être que la loi. Au contraire, la plupart des recommandations sont susceptibles d'être interprétées comme pouvant donner lieu, ou bien à une traduction juridique contraignante, ou bien à une appropriation volontaire de la part des acteurs, plusieurs degrés étant envisageables entre ces deux extrêmes.

Deux principes fondateurs ressortent de cette réflexion. Il convient d'y insister tout particulièrement, tant ils sont susceptibles de subsumer quelques-uns des défis éthiques majeurs soulevés par l'intelligence artificielle.

D'une part, **un principe substantiel, le principe de loyauté des algorithmes,** dans une formulation approfondissant celle déjà élaborée par le Conseil d'Etat (voir section « Le principe de loyauté »). Cette formulation intègre en effet une dimension de loyauté envers les utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens, voire envers des collectifs, des communautés dont l'existence pourrait être affectée par des algorithmes, que ceux-ci d'ailleurs traitent des données personnelles ou pas.

D'autre part, **un principe plus méthodologique : le principe de vigilance.** Ce principe de vigilance doit être entendu, non comme une vague incantation mais comme une réponse étayée à trois enjeux centraux de la société numérique. Premièrement, le caractère évolutif et imprévisible des algorithmes à l'ère de l'apprentissage automatique (machine learning). Deuxièmement, le caractère très compartimenté des chaînes algorithmiques, induisant segmentation de l'action, indifférence aux impacts générés par le système algorithmique dans son ensemble, dilution des responsabilités. Troisièmement, enfin, le risque d'une confiance excessive accordée à la machine, jugée – sous l'effet d'une forme de biais cognitif humain – infaillible et exempte de biais. À travers le principe de vigilance, l'objectif poursuivi est en somme d'organiser l'état de veille permanente de nos sociétés à l'égard de ces objets socio-techniques complexes et mouvants que sont les algorithmes ou, à proprement parler, les systèmes ou chaînes algorithmiques. Un état de veille, autrement dit un questionnement, un doute méthodique. Ceci concerne au premier chef les individus qui composent les maillons des chaînes algorithmiques : il s'agit de leur donner les moyens d'être les veilleurs, lucides et actifs, toujours en questionnement, de cette société numérique. Ceci concerne aussi les autres forces vives de notre société. Les entreprises, bien sûr, pour modeler des systèmes algorithmiques vertueux, mais pas seulement.

Ces principes, par la démarche universelle dont ils procèdent, pourraient bien s'inscrire dans une nouvelle génération de principes et de droits de l'homme à l'ère numérique : cette génération qui après celles des droits-libertés, des droits patrimoniaux et des droits sociaux, serait celle des droits-système organisant la dimension sous-jacente à notre univers numérique. Ne sont-ils pas susceptibles d'être portés au niveau des principes généraux de gouvernance mondiale de l'infrastructure internet ? À l'heure où se construisent les positions française et européenne sur l'intelligence artificielle, la question mérite d'être posée.

Les principes de loyauté et de vigilance pourraient s'inscrire dans une nouvelle génération de principes et de droits de l'homme à l'ère numérique : des droits-système organisant la dimension sous-jacente à notre univers numérique

ANNEXES

Les applications et les promesses des algorithmes et de l'IA

Les pages qui suivent n'ont pas vocation à développer une vision critique. Il s'agit plutôt ici de décrire les grands usages des algorithmes et de l'IA déjà à l'œuvre ainsi que, dans un ordre plus prospectif, certaines promesses aujourd'hui évoquées principalement par des acteurs dont la posture n'est pas toujours neutre. Il convient de garder à l'esprit qu'une part non négligeable du discours public sur les algorithmes et l'IA – souvent la plus irénique et parfois la plus catastrophiste – est déterminée par des intérêts commerciaux.

Santé

L'outil algorithmique fait l'objet de larges promesses. Comme dans chaque secteur, les opportunités dans le champ de la santé doivent cependant être appréhendées avec prudence, notamment du fait des immenses capacités « marketing » des organisations qui les déploient[68]. Le rôle annoncé et parfois déjà effectif des algorithmes et de l'IA dans le domaine de la santé est indissociable de l'existence de bases de données de plus en plus massives, tant en termes d'individus concernés qu'en terme de quantité de données disponibles sur chacun d'eux. **L'algorithme et l'IA permettent justement de tirer parti de cette quantité inédite de données disponibles aujourd'hui** (données issues des grandes bases médico-administratives rassemblées dans le SNDS[69] mais aussi des objets de santé connectée, des dossiers de patients, etc.) pour bâtir des modèles au sein desquels un profil très précis de chaque individu peut être dessiné, ce profil pouvant constituer le soubassement d'une prévision.

Ces promesses, qui concernent les grands objectifs de santé publique, concernent d'abord l'idée d'**une médecine à la fois prédictive, préventive et personnalisée.** L'analyse et la confrontation de mon profil génomique à celui d'individus similaires et à leurs parcours de santé peuvent aider au **diagnostic précoce.** Elles peuvent aussi permettre d'évaluer mes chances de développer telle ou telle maladie (cancer, diabète, asthme etc.), de « prédire » en quelque sorte ma santé future et dès lors m'inciter à prendre des mesures en conséquence (grâce à des campagnes de prévention ciblées). L'établissement de profils biologiques affinés permettrait également de **personnaliser les traitements et stratégies thérapeutiques.**

> **L'intelligence artificielle se développe notamment en cancérologie. L'un des exemples les plus fréquemment mentionnés à cet égard est celui de Watson, d'IBM. Watson analyse en effet les données génétiques des patients, les informations les concernant recueillies lors de leur admission, leur historique médical et les compare avec 20 millions de données issues d'études d'oncologie clinique pour établir un diagnostic et proposer un traitement. L'école de médecine de l'Université de Caroline du Nord a ainsi conduit en octobre 2016 une expérience montrant que les préconisations de Watson recoupaient les traitements prescrits par les cancérologues dans 99% des 1000 cas de cancer étudiés. Cette expérience a aussi démontré que dans 30% des cas, Watson était à même de proposer davantage d'options thérapeutiques que les médecins. Il convient toutefois de considérer avec prudence ces résultats annoncés, par ailleurs promus avec d'importants moyens de communication et de relations publiques.**

68 Gérard Friedlander, doyen de la faculté de médecine de l'Université Paris Descartes, l'a notamment souligné (événement organisé par l'Hôpital Necker et l'Institut Imagine, le 15 septembre 2017)

69 Système national des données de santé.

Outre la capacité d'une médecine de plus en plus appuyée sur les algorithmes et sur l'IA à faire fonds sur l'ensemble des variables biologiques, comportementales et environnementales, son intérêt réside aussi dans sa **capacité à traiter une masse d'informations scientifiques et de recherche qu'aucun médecin n'aurait matériellement la possibilité de maîtriser** (à titre d'exemple, on dénombre pas moins de 160 000 publications par an en cancérologie) dans la perspective de formuler un diagnostic.

L'intelligence artificielle est aussi susceptible de fournir un **appui à la détection de risques sanitaires. Les algorithmes peuvent être utiles pour « repérer l'élévation de l'incidence de maladies ou de comportements à risque, et d'alerter les autorités sanitaires[70] »**. Par exemple, en France, les liens entre l'utilisation d'une pilule contraceptive de 3ème génération et le risque d'AVC a pu être étudié grâce au traitement algorithmique de la base du Système national des données de santé (SNDS). La mise en œuvre d'un algorithme peut aussi permettre de **prédire des risques de maltraitance.** Il faut d'ailleurs souligner que ce n'est pas là un fait nouveau. Déjà en 1981, la CNIL avait eu à connaître d'un projet du Ministère de la Santé et des Affaires sociales visant à automatiser le signalement d'enfants présentant des risques psycho-sociaux (fichier GAMIN) : sur la base de l'analyse de 70 données différentes, le système devait repérer les cas à examiner en priorité. C'était bien un modèle, matérialisé par une série de critères, que l'algorithme permettait d'appliquer automatiquement à de très vastes cohortes.

Dans la pratique médicale, les algorithmes sont à certains égards déjà bien implantés pour **automatiser des tâches du quotidien.** Les logiciels d'aide à la prescription (LAP), une fois une maladie déjà diagnostiquée, sont déjà de précieux outils d'aide à la décision pour les médecins au moment de la saisie d'ordonnances. Ils permettent d'utiliser le dossier d'un patient pour repérer des contre-indications, des allergies ou des interactions médicamenteuses dangereuses. Autres applications déjà bien inscrites dans le paysage médical : « l'analyse d'image (imagerie médicale, anatomo-pathologie, dermatologie), l'analyse de signaux physiologiques (électro-cardiogramme, électro-encéphalogramme) ou biologiques (séquençage de génome) »[71]. L'utilité de l'IA est également mise aujourd'hui en avant pour **optimiser la mise en place d'essais cliniques grâce à une automatisation de la sélection des patients.**

En somme, sous réserve de précautions, l'algorithme en santé permettrait de mieux à répondre à certains besoins « pour les médecins (plus de sécurité), pour les patients (plus de personnalisation), et pour les instances publiques (plus de rationalisation) »[72].

Éducation

L'application désormais la plus connue des algorithmes dans le domaine de l'éducation a trait à l'**affectation des immenses effectifs que doit gérer chaque année l'administration de l'Education nationale** et à l'attribution de places en lycée et dans le supérieur en fonction des vœux formulés par les candidats.

Le cas de l'algorithme « APB » (Admission post-bac) a été particulièrement évoqué depuis l'été 2016. Déployé depuis 2009 afin de faciliter et de fluidifier l'appariement entre les souhaits des élèves émis sous la forme de vœux et les places disponibles dans l'enseignement supérieur, il concernait en 2017 environ 808 000 inscrits dont 607 000 élèves de Terminale ayant candidaté aux 12 000 formations disponibles sur le logiciel. Pour que le système fonctionne, des critères de priorité ont été établis, pour être appliqués à tous. L'objectif poursuivi par APB, et sans évoquer à ce stade les critiques auxquelles il a pu donner lieu, étant double. D'une part, il s'agissait d'automatiser une tâche immense et donc d'optimiser un processus administratif particulièrement coûteux en temps. D'autre part, APB est aussi crédité d'avoir amélioré un fonctionnement qui laissait auparavant la place à des formes d'arbitraire. Roger-François Gauthier, expert des politiques éducatives, explique ainsi que les algorithmes tels qu'APB ou AFELNET (pour la répartition des élèves en lycée) « ont fait quelque chose de remarquable : ils ont mis fin à un fonctionnement mafieux. Auparavant, ces décisions de répartition se prenaient dans le secret des bureaux des proviseurs et des inspecteurs d'académie avec des piles de recommandations ».

En plus d'être efficace, l'algorithme est donc présenté comme assurant l'équité et la non-manipulabilité (chaque lycéen devant effectuer ses choix sans autocensure) puisque la décision est prise de façon automatique, en fonction des données du candidat, de ses vœux d'affectation et selon des critères identiques pour tous puisque programmés une fois pour toutes lors du paramétrage de l'algorithme.

L'autre grand champ d'application des algorithmes (y compris de l'IA) dans l'éducation concerne directement les pratiques pédagogiques elles-mêmes. On s'y réfère souvent sous le titre de *learning analytics*. Ici encore le recours aux algorithmes est indissociable de la capacité inédite à collecter des données extrêmement nombreuses et diversifiées : données d'apprentissage (sur les résultats aux exercices mais potentiellement aussi sur la manière dont l'élève s'y confronte, durée de résolution), données sur les interactions avec l'enseignant et avec les pairs, données socio-démographiques, etc.

70 INSERM, dossier d'information « Big data en santé » (disponible en ligne)
71 Evénement organisé par le Conseil départemental du Rhône de l'Ordre des médecins, le 28 septembre 2017.
72 Evénement organisé par le Conseil départemental du Rhône de l'Ordre des médecins, le 28 septembre 2017.

L'analyse des données sur l'apprentissage des élèves à l'aide d'algorithmes et de systèmes d'intelligence artificielle est aujourd'hui conçue comme le moyen de développer des stratégies de personnalisation de l'enseignement. On retrouve ici, comme dans le domaine médical abordé précédemment, la possibilité de la détermination d'un profil très fin de chaque élève mis à profit pour « diagnostiquer » une situation d'apprentissage, pour détecter un éventuel décrochage scolaire mais aussi pour permettre l'élaboration de stratégies individuelles d'apprentissage et de formation, adaptées au profil de chaque élève. La consultation en ligne organisée dans le cadre du débat public par le NumériLab (au sein du Ministère de l'Education Nationale) aborde les intérêts que pourraient revêtir les *learning analytics* pour la communauté éducative. Dans un contexte français où la différenciation pédagogique par « groupes de besoin » est loin d'être effective, certains contributeurs voient dans l'algorithme la possibilité de « mettre en œuvre des situations individuelles et collectives qui tiennent compte des différentes difficultés rencontrées par les élèves, leur permettre d'avoir des parcours individualisés, rendre compte de leur évolution et les faire partager à l'ensemble de la communauté éducative ».

Vie de la cité et politique

Les algorithmes et l'intelligence artificielle investissent également le champ de la politique, au double sens du terme, c'est-à-dire tant en ce qui concerne l'organisation de la cité (les politiques publiques) que les pratiques de conquête du pouvoir, la vie électorale.

Le cas, précédemment évoqué, de l'algorithme APB en fournit un exemple. D'autres exemples sont peut-être moins attendus dans la mesure où il peut s'agir d'algorithmes déployés non pas par des administrations mais par des entreprises privées dont l'activité peut avoir un impact direct sur des domaines relevant généralement de l'autorité publique. Des applications de géolocalisation et de guidage routier mises à disposition des automobilistes peuvent modifier sensiblement les flux de circulation dans une ville et illustrent donc pleinement l'impact des algorithmes sur la vie collective. Dans un autre ordre d'idées, **la place cruciale que prennent désormais les algorithmes dans la recherche et le filtrage de l'information** les situent à un point névralgique de la vie démocratique. Les algorithmes de reconnaissance et le *machine learning* améliorent également l'efficacité de la modération automatique de propos déplacés sur les réseaux sociaux ou autres sites hébergeant des contenus : la DGMIC évoque l'ouverture par des sites de presse de leurs articles aux commentaires, l'algorithme permettant ici de favoriser le débat et l'exercice du pluralisme.

Au cours des dernières années, d'abord aux Etats-Unis, des offres de **logiciels d'aide à la stratégie électorale** se sont développées. Beaucoup de ces solutions reposent en fait sur la mise en œuvre d'algorithmes prédictifs qui analysent les données électorales. On retrouve ici, une fois encore, l'association entre la capacité des grandes quantités de données et celle – précisément par le biais de l'algorithme – à les exploiter, à les « faire parler » en construisant un modèle à partir de l'analyse des données passées qui est ensuite appliqué aux données actuelles pour élaborer enfin des recommandations, une aide à la décision stratégique.

Le logiciel 50+1 déployé depuis 2012 par la société LMP sur le fondement d'une expertise acquise pendant la campagne électorale américaine de 2008 en offre un bon exemple. Son objet est d'accompagner les stratégies électorales des candidats aux élections politiques en leur indiquant les zones à faire cibler en priorité par leurs équipes de militants pour des actions de porte-à-porte. L'algorithme intervient pour analyser les données des élections passées (résultats électoraux bureau de vote par bureau de vote, données socio-démographiques), en inférer un modèle qui, appliqué à la circonscription faisant l'objet de la campagne du candidat utilisateur du logiciel, permette in fine de formuler une prédiction sur la tendance dans l'aire de chaque bureau de vote. Outre l'intérêt que peut présenter ce type de logiciel pour les candidats aux élections, ses promoteurs le présentent également comme un moyen de lutter contre l'abstention dans le cadre d'une stratégie visant à remobiliser les abstentionnistes.

Si la législation française sur la protection des données personnelles ne permet pas le déploiement de logiciels qui cibleraient individuellement les électeurs (à l'exception de ceux y ayant consenti), le terrain électoral américain est un observatoire d'applications des algorithmes et de l'intelligence artificielle à des fins de profilage individuel[73]. Les deux campagnes présidentielles menées par Barack Obama ont vu se déployer de telles campagnes de marketing ciblé. La stratégie électorale de Donald Trump en 2016 semble avoir vu le franchissement d'un nouveau seuil dans le recours à ce type d'outils de communication ciblée[74], appuyés sur le recours à des données issues des réseaux sociaux et des courtiers en données. Même si de fortes incertitudes demeurent sur la réalité de ces pratiques, l'envoi de milliers de messages extrêmement individualisés (en fonction des préoccupations et attentes inférées du profil de chaque électeur) au cours d'une même soirée a pu être évoqué[75].

73 Une autre manière de présenter ces applications est de souligner qu'elles permettent une « prédiction » de ce que pourrait être le comportement d'un électeur ou encore une « recommandation » adressée à l'utilisateur du logiciel quant au type d'action requise en fonction du profil (envoi de tel message, utilisation préférentielle de tel canal de communication).

74 En France, les prédictions et recommandations d'un logiciel tel que 50+1 concernent des cohortes de 1000 personnes et ne relèvent donc pas d'outils de ciblage individuel.

75 https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage

Culture et médias

L'utilisation d'algorithmes et d'intelligence artificielle produit déjà de forts impacts sur la structuration de l'offre de produits culturels et, partant, probablement aussi sur les pratiques de consommation culturelle. **Différents services de recommandation** facilitent la hiérarchisation de l'information « afin de répondre au besoin de l'utilisateur de s'orienter dans la surabondance des contenus accessibles »[76]. Le recours à ces services de « matching » concerne, à des degrés de développement variables selon la DGMIC, des secteurs très divers au sein de l'industrie culturelle : la vidéo à la demande par abonnement (80 % des contenus visionnés sur Netflix seraient issus de recommandations personnalisées), la musique (la fonctionnalité de recommandation apparaît comme un réel enjeu de différenciation pour des services de streaming tels que Spotify ou Deezer), les services gratuits (pour Facebook, Youtube ou encore Google, l'algorithme participe à la maximisation du nombre d'utilisateurs et ainsi à leur exposition augmentée à la publicité) ou encore les sites de commerces en ligne (30% des ventes d'Amazon résulteraient de ses recommandations algorithmiques).

L'intérêt de tels services est triple : tout d'abord, ils permettent de proposer au client une relation plus individualisée qui accompagne éventuellement la découverte d'autres offres. Ils peuvent également profiter à l'industrie audiovisuelle ou culturelle dans la mesure où ils facilitent *« la découverte d'œuvres audiovisuelles qui ne seraient pas par ailleurs programmées en raison de leur petit budget, ou en raison de l'absence d'un distributeur ou d'un budget de promotion ».* En effet, *« grâce aux moteurs de recommandation, certains films peuvent trouver un public même si ces films ne sont pas programmés par les chaînes de télévision traditionnelles »*[77]. Enfin – et peut-être, surtout – l'enjeu économique est indéniable pour fournisseurs et plateformes qui, en orientant les usagers, augmentent la satisfaction et ainsi l'utilisation de leur service.

Toutefois, il convient de nuancer les implications de l'algorithme sur le secteur. La DGMIC, qui s'appuie sur les auditions d'une quinzaine d'acteurs du secteur, indique que *« la recommandation personnalisée n'a pas tenu toutes ses promesses et que, bien que cette fonction apparaisse aujourd'hui incontournable à l'utilisateur, ce n'est pas celle qui guide majoritairement la consultation et la consommation des contenus »,* le travail des équipes éditoriales demeurant fondamental. En fonction du perfectionnement futur des algorithmes, la recommandation pourrait néanmoins occuper une place encore plus prépondérante dans les industries culturelles. A titre d'exemple, la startup Prizm commercialise des enceintes qui, en combinant des informations sur le moment de la journée, l'ambiance ou le nombre de personnes dans la pièce, diffusent la playlist la plus adéquate.

Ces algorithmes agissent sur le fondement de trois types de données : des données personnelles attachées aux profils des utilisateurs (l'historique d'usage par exemple), des données attachées aux œuvres (mots-clés indexés tantôt manuellement tantôt, depuis peu, de manière automatique) et, plus rarement, des données contextuelles (l'heure d'écoute ou la météorologie, par exemple). La recommandation peut s'exercer selon trois logiques différentes : tout d'abord, un filtrage sémantique peut viser à *« placer l'utilisateur sur la « cartographie » des **contenus »*** (DGMIC) sur la base notamment de son historique ou de questionnaires visant à mieux comprendre ses goûts. Une autre approche plus souvent privilégiée, celle du **filtrage collaboratif,** consiste à recommander en partant de l'hypothèse que deux utilisateurs partageant un avis sur un contenu sont plus susceptibles d'être également en accord sur un autre contenu plutôt que deux utilisateurs choisis aléatoirement. Le filtrage collaboratif peut se fonder autant sur le comportement des utilisateurs, leurs consommations passées *(« les utilisateurs ayant aimé le contenu A ont aussi aimé le contenu B »)* que sur l'objet directement *(« si Alice aime les contenus a, b, c et d, et que Benoit aime a, b et c, il est cohérent de recommander d à ce dernier »).* Enfin, un **filtrage hybride** permet de combiner ces deux méthodes pour optimiser la performance de recommandation. Ainsi, l'algorithme de recommandation de Spotify opère de la façon suivante[78] :

- En premier lieu, les contenus écoutés (style, tempo) sont analysés (soit plutôt une approche basée sur les contenus) ;
- Ensuite, les genres musicaux les plus appréciés sont regroupés en fonction de ceux des autres utilisateurs ayant consommé les mêmes contenus ;
- Enfin, l'utilisateur est circonscrit par rapport à ses propres comportements et son profil (type de consommation, fréquence d'écoute etc.).

Autre exemple d'algorithmes dans le champ de la culture : bien qu'embryonnaire, la **génération automatique de contenus culturels,** afin de produire et imiter les contenus qui plaisent, constitue une idée qui séduit. La DGMIC précise néanmoins que *« les nombreuses tentatives de prédiction du succès d'un livre ou d'un scénario déjà écrit grâce à des algorithmes n'ont pour l'instant pas permis de découvrir le secret le plus convoité des industries culturelles, industries de prototypes et de risques ».*

76 DGMIC (Ministère de la Culture), « Les algorithmes dans les médias et les industries culturelles »
77 Rapport du CSA Lab, p.14
78 CNIL, « Les données, muses et frontières de la création », Cahier IP n°03, octobre 2015

Justice

Des évolutions majeures sont à l'œuvre dans l'exercice des métiers du droit et de la justice. Si la plupart n'en sont qu'à un stade de développement anticipé, l'intérêt suscité par les outils technologiques recourant aux algorithmes est grand. L'algorithme peut tout d'abord permettre pour l'avocat ou le juge d'**obtenir un appui pour des tâches très variées désormais automatisables,** souvent répétitives voire laborieuses : « *l'évaluation des éléments de preuve selon différentes méthodes (fiabilité des témoins oculaires, distinction des rumeurs et des témoignages, procédures de discovery, constructions d'explications alternatives), la modélisation du travail des jurys, l'extraction d'informations contenues dans des documents (data mining), l'interprétation des informations (mise en lumière de modèles ou d'associations possibles, hiérarchisation des informations…), la recherche d'informations, la construction d'une argumentation (modélisation de structures d'argumentations, utilisation d'arbres de raisonnements permettant de lier une demande, aux justifications et objections dont elle peut faire l'objet), l'élaboration de documents, de formulaires juridiques et de contrats, ou encore la résolution de différends* »[79]. C'est cependant les promesses de la **justice dite « prédictive » ou « prévisionnelle »** qui méritent le plus d'attention tant elles pourraient bouleverser la conception « humaniste » de la justice. Elle peut être définie comme l'« outil informatique, reposant sur une base de données jurisprudentielles, qui, à l'aide d'algorithmes de tri et (pour les plus perfectionnés) de « réseaux neuronaux », va permettre d'anticiper quelles seront les statistiques de succès de tel ou tel argument juridique »[80].

La possibilité d'une justice prévisionnelle a été conditionnée par la présence de **bases de données jurisprudentielles** toujours plus fournies. Si elles n'étaient auparavant pas mises à la disposition de tous, la loi dite « République Numérique » a favorisé la diffusion des décisions de justice administrative et judiciaire par le mouvement d'ouverture des données publiques (open data) qu'elle consacre. De nombreuses start-ups[81] se saisissent ainsi depuis plusieurs mois de cette nouvelle masse de données pour développer leurs outils de « justice prévisionnelle » dont l'objectif principal est de repérer des récurrences à des fins de prédiction. Les intérêts et exploitations potentiels sont multiformes et recouvre différents champs des métiers du droit, du juriste à l'avocat en passant par le juge.

Pour le **justiciable et les professionnels du droit,** les logiciels algorithmiques peuvent être d'une utilité stratégique en optimisant l'**identification des solutions statistiquement les plus probables pour un contentieux donné** ou le montant prévisible des dommages-intérêts. Cette méthode est notamment adaptée aux contentieux particulièrement propices aux récurrences, tels que le licenciement sans cause réelle et sérieuse ou les prestations compensatoires en cas de divorce. Si ces outils se généralisent au sein des différentes professions du droit, ils contribueraient au dessein plus général d'une « smartjustice », à savoir une justice animée par des impératifs de meilleure rentabilité avec le minimum de moyens, grâce aux technologies. L'avocat pourrait bénéficier d'un gain significatif de temps – et ainsi se consacrer à des tâches plus gratifiantes d'analyse juridique et de contact humain –, tandis que le justiciable pourrait éviter certains coûts, en faisant le choix de s'entendre à l'amiable plutôt que de saisir le juge dans des cas où les chances du succès d'un procès sont réduites. Pour le fonctionnement du système de justice français dans son ensemble de surcroît, un recours grandissant à ces solutions annoncerait une diminution du nombre de saisines et un certain désengorgement des juridictions, éventualité plus qu'attrayante dans le contexte actuel.

Parallèlement, les algorithmes prédictifs peuvent être une **ressource utile au juge :** s'inspirer des recommandations de la « machine », fondées sur les jurisprudences précédentes, lui permettrait d'éclairer ses décisions. C'est l'ambition d'une qualité de la justice augmentée et de l'**harmonisation des décisions** qui serait au cœur de ce modèle. En d'autres termes, dans la continuité de mesures récentes telles que les barèmes, la « justice prévisionnelle » réduirait l'horizon d'incertitude et participerait à l'évaluation interne des juridictions et magistrats.

L'aide à la décision fondée sur des algorithmes au service du juge a fait l'objet d'une expérimentation cette année par les cours d'appel de Rennes et Douai en partenariat avec le ministère de la Justice. Par un communiqué du 9 octobre 2017, le ministère a annoncé que l'outil développé par la start-up Predictice ne s'était pas avéré satisfaisant. De futures expérimentations sont néanmoins prévues, aux prochains stades du développement de l'outil.

Le mouvement d'open data n'en est qu'à ses premiers frémissements : toutes les conditions sont ainsi réunies pour que la justice prévisionnelle prolifère, dans un contexte où 1,5 million de décisions seront désormais « anonymisables » chaque année et ainsi mises à disposition sur Jurinet (base interne de la Cour de cassation) et Légifrance.

79 Contribution au débat public d'un groupe de travail du Conseil National des Barreaux.
80 BOUCQ Romain, « La justice prédictive en question », Dalloz Actualité, 14 juin 2017.
81 Predictice, Case Law Analytics ou encore Doctrine.fr constituent des exemples de telles *legaltech*.

Banque, Finance

Plusieurs événements récents ont contribué à accroître l'attention publique accordée à l'utilisation d'algorithmes dans le champ financier. Même si le rôle effectif joué par l'algorithme dans le flash crash du 6 mai 2010 pose débat, la chute historique du Dow Jones (environ 9%) a largement interpellé quant aux risques d'emballement, de manipulation et de comportements moutonniers associés à ce qui est aujourd'hui désigné sous l'appellation **« trading haute fréquence »** (THF). Un autre exemple est celui du piratage du compte Twitter de l'agence Associated Press en avril 2013 : en surveillant les mots-clefs figurant sur le réseau social, les algorithmes ont conclu à un attentat à la Maison blanche, précipitant ainsi le retrait de milliards d'ordres sur les marchés en quelques secondes.

Aussi appelé *speed trading* ou trading algorithmique, le THF désigne l'**automatisation d'arbitrages boursiers** qui connaît une ascension fulgurante depuis la fin des années 1990. La directive dite « MIF II »[82], qui encadre cette tendance et qui entrera pleinement en application en janvier 2018, définit le THF comme *« la négociation d'instruments financiers dans laquelle un algorithme informatique détermine automatiquement les différents paramètres des ordres [...] avec une intervention humaine limitée ou sans intervention humaine »* (article 4, paragraphe 39). Ce négoce financier d'un genre nouveau voit ainsi des robots traders d'une rapidité remarquable se substituer aux traditionnels « teneurs de marchés ». Prendre des décisions d'investissement et organiser les liquidités ne constituent désormais plus l'apanage de l'humain : le robot serait impliqué dans près de 70 % des transactions aux Etats-Unis et environ 40 % de celles en Europe. L'algorithme jalonne désormais le processus d'investissement, d'abord en amont par l'identification des opportunités, puis en aval par les règles opératoires d'exécution qui prennent position à l'achat ou à la vente[83]. Peu de problématiques inédites semblent finalement avoir émergé depuis une quinzaine d'années, et le THF a déjà fait l'objet d'un important effort de régulation et de responsabilisation des acteurs[84].

Si un tel intérêt pour l'automatisation s'est manifesté depuis 1995, année de création du THF, c'est parce qu'il redéfinit radicalement la temporalité de la bourse : dans ce secteur, l'ampleur de l'écart entre performance humaine et performance technologique est incontestable. Cette vélocité implique un second intérêt de taille pour les acteurs du THF (gestionnaires de fonds, institutions bancaires)[85] qui, en mettant en œuvre des stratégies d'investissement irréalisables manuellement, voient leurs profits et leur compétitivité croître de manière substantielle.

L'algorithme dans le champ de la finance, c'est également l'émergence de « robo-advisors » visant à **automatiser les services financiers** fournis aux clients et la gestion de leurs portefeuilles. Leur niveau de maturité semble néanmoins à ce stade assez faible selon l'Autorité des marchés financiers. Plus facilement mobilisables aujourd'hui, des outils basés sur des algorithmes visent à **automatiser la gestion des risques** et le contrôle de la conformité (la lutte anti-blanchiment, par exemple). Enfin, la personnalisation permise par l'algorithme pourrait mener à des mutations importantes des services financiers proposés aux clients : et si, à terme, une segmentation s'opérait entre une clientèle réduite qui aurait accès à des produits très sophistiqués comparativement à une autre qui se verrait proposer un éventail très réduit de produits simples ?

Sécurité, défense

Le recours aux algorithmes dans le domaine de la sécurité et de la défense a pour finalités principales annoncées l'identification de suspects, la prédiction de commission d'infractions et l'automatisation d'opérations de maintien de l'ordre voire de guerre, jusqu'à l'acte de tuer, cette dernière finalité faisant l'objet d'un vif débat international.

Les années 2000 ont vu converger accroissement de la menace terroriste dans le sillage du 11 septembre 2001 et de l'explosion du nombre de données disponibles (liée à la numérisation globale des sociétés). Le problème, classique pour le renseignement, de l'analyse et de l'exploitation des données disponibles s'en trouve accru. Dans un contexte d'exigence politique très forte à l'égard des services de renseignement, les algorithmes sont présentés – à tort ou à raison – comme une solution permettant d'identifier les suspects en tirant pleinement partie des données disponibles. Le système API-PNR ou les « boîtes noires » évoquées lors de la discussion de la loi sur le renseignement de 2015 relèvent de cette logique. Les données des passagers aériens, dans un cas, celles de l'ensemble de la population, dans l'autre, sont filtrées par des algorithmes à la recherche de « signaux faibles », de profils considérés comme suspects en fonction de critères tenus secrets.

L'essor de l'idée de **« police prédictive »** correspond à l'idée de prédire la commission d'infractions au moyen de l'analyse massive de données concernant la commission passée de crimes et de délits afin de répartir plus efficacement les patrouilles. La promesse portée par exemple par le logiciel américain « Predpol » est d'adosser les méthodes policières traditionnelles jugées trop subjectives par des méthodes considérées comme « objectives ».

82 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers.
83 Benghozi P.-J., Bergadaà M., Gueroui F., Les temporalités du web, 2014, chapitre 3 «Trading haute fréquence : l'arbitre sans sifflet ».
84 Directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 ; loi n° 2013-672 du 26 juillet 2013 de séparation et de régulation des activités bancaires.
85 Getco, Flow traders, IMC, Quantlab, Optiver...

Ces initiatives soulèvent pourtant d'importantes critiques. Le sociologue Bilel Benbouzid conteste ainsi à propos du logiciel « PredPol » la pertinence de l'application à la criminalité de logiques empruntées à la sismologie. L'attrait présenté par « Predpol » aux yeux de décideurs tiendrait en revanche à ce que ce type d'outils permet de *« gérer, selon des critères gestionnaires, l'offre publique de vigilance quotidienne »*[86]. Par ailleurs, leurs résultats concrets semblent pour l'heure décevants aux praticiens eux-mêmes. Par exemple, l'expérimentation « PredVol » visant la prédiction des actes de délinquance commis sur les véhicules aboutit « à faire ressortir toujours les mêmes spots, les mêmes points chauds aux mêmes endroits » selon le Colonel Philippe Mirabaud. Aussi, l'étude des vols avec violence sans arme contre les femmes sur la voie publique à Paris[87] révèle la forte régularité de ces actes – aussi bien en termes de localisation que d'horaires – mais les possibilités prédictives restent limitées. Ce constat repose en partie sur les difficultés à « faire parler » des jeux de données encore disparates. La plupart des outils dits « prédictifs » s'appuient sur les données des préfectures de police – plaintes des victimes et/ou arrestations notamment – dont l'utilisation à des fins de prédiction est loin d'être naturelle. Le perfectionnement de ces logiciels implique de les compléter par des données externes concernant autant le terrain des actes (densité de bars ou commerces, présence d'une station de métro etc.) que les conditions météorologiques ou encore les événements organisés au sein d'une ville par exemple.

Les experts invitent à ne pas sombrer dans le fétichisme technologique en pensant que l'algorithme aurait la capacité d'apporter une solution magique aux enjeux de sécurité. Gilles Dowek explique ainsi que « même avec un système d'une performance extrêmement élevée, il y aura toujours beaucoup plus d'innocents que de coupables accusés. Supposons un algorithme d'une super-qualité qui n'a qu'une chance sur 100 de se tromper. Sur 60 millions de personnes, ça fait 600 000 personnes détectées à tort, plus les 1 000 « vrais positifs » qu'on a bien détectés. Donc l'algorithme détecte 601 000 personnes, parmi lesquelles en réalité 1 000 seulement sont de vrais terroristes ». Le risque est donc de démultiplier la suspicion et de confronter les services de renseignement à une masse de cibles impossible à traiter.

Au-delà de l'identification de zones à risque, l'algorithme peut servir d'**aide à la résolution des enquêtes.** En s'appuyant sur les connexions entre l'ensemble des pièces d'une enquête – dont celles au caractère très technique comme procès-verbaux, appels téléphoniques ou encore informations bancaires –, des logiciels offriraient aux gendarmes la possibilité d'identifier des relations que l'humain n'était jusqu'ici pas parvenu à effectuer[89].

Si tout invite à modérer l'enthousiasme des promoteurs de la police prédictive, des perspectives intéressantes résident dans l'appui à la contextualisation, à l'interprétation et ainsi à l'organisation. Hunchlab, projet de l'entreprise Azavea, œuvre ainsi en ce sens en accentuant l'effort d'intelligibilité quant à ce que la prédiction permet ou ne permet pas, par une rétroaction plus solide et une interaction plus forte entre l'humain et l'outil. Dans tous les cas, s'il est difficile de préciser les contours des futures solutions privilégiées et malgré des réserves au sein de la communauté scientifique, les pouvoirs publics n'excluent pas d'y avoir recours pour *« la constitution d'une aide à la décision (« analyse décisionnelle »), au profit du commandant d'unité territoriale, notamment à des fins de prévention de la délinquance »*[90].

Extrêmement sensible est enfin la question posée par le **développement d'armes létales autonomes (robots tueurs)** qui pourraient prendre elles-mêmes la décision de tuer sur le champ de bataille ou à des fins de maintien de l'ordre. De tels systèmes sont déjà déployés à la frontière entre les deux Corée et les armées de divers pays réfléchissent actuellement à la mise en service de drones tueurs capables d'engager et d'éliminer une cible sans intervention humaine. En 2015, une pétition signée par plus d'un millier de personnalités, dont une majorité de chercheurs en IA et en robotique, ont réclamé l'interdiction des armes autonomes, capables *« de sélectionner et de combattre des cibles sans intervention humaine »*. Cette initiative a donné de la visibilité à un débat international déjà engagé à l'ONU.

Assurance

Les algorithmes offrent tout d'abord au secteur assurantiel la possibilité d'accélérer et de **fluidifier des pratiques quotidiennes** telles que la gestion des sinistres, le suivi du comportement des assurés, leur indemnisation ou encore la lutte contre la fraude. La reconnaissance d'images permise par l'IA pourrait mener à systématiser, grâce à l'analyse des images de sinistres, les processus d'indemnisation « auto » et habitation . Autre exemple : l'intelligence artificielle, en révélant des liens insoupçonnés, peut se révéler utile pour retrouver les titulaires de contrats d'assurances-vie en déshérence (non réclamés) ou leurs héritiers. Mais, plus qu'un instrument d'automatisation au service de pratiques déjà bien implantées, l'algorithme annonce un nouveau paradigme de l'assurance et du mutualisme au sens où il pourrait *« modifier la manière d'appréhender les risques et de les valoriser, transformer les techniques et les pratiques de mutualisation »* (François Ewald[92]).

Certes la donnée a toujours constitué la matière première pour l'assureur pour prévenir les risques. Assurer, c'est pro-

86 Bilel Benbouzid, « A qui profite le crime ? », *La Vie des Idées.* « PredPol » prétend s'inspirer des méthodes de prédiction des tremblements de terre pour offrir une « analyse du crime en temps réel qui prend la forme d'un tableau de bord ».
87 Le géostaticien Jean-Luc Besson l'a exposée lors du même événement organisé par l'INHESJ.
88 http://tempsreel.nouvelobs.com/rue89/rue89-internet/20150415.RUE8669/l-algorithme-du-gouvernement-sera-intrusif-et-inefficace-on-vous-le-prouve.html
89 Le loigiciel AnaCrime a ainsi permis il y a quelques mois de relancer l' « affaire Gregory ».
90 Réponse du Ministère de l'Intérieur à la question n°16562, publiée dans le JO Sénat du 29 décembre 2016.
91 Evénement organisé par la Fédération Française de l'Assurance, le 5 juillet 2017.
92 François Ewald, « After Risk, vers un nouveau paradigme de l'assurance. L'Assurance à l'âge du Big Data », septembre 2013.

poser des services financiers de protection différents selon des profils de risque, grâce au traitement de données à caractère prédictif. Florence Picard (Institut des actuaires)[93] explique ainsi comment l'actuaire a toujours eu pour rôle de de calculer la probabilité et l'impact financier des risques. Loin de l'appréciation globale fondée sur les déclarations des clients, l'algorithme annonce une évaluation plus fine s'appuyant sur des données comportementales en masse.

Objets connectés, réseaux sociaux, données de santé : de nouveaux horizons s'ouvrent vers une personnalisation sans précédent. Ce sont des corrélations inédites et individualisées qui sont ici recherchées. A titre d'exemple, certains assureurs auraient constaté que les clients achetant des feutres à placer sous les pieds de table et de chaise, pour la préservation du bon état de leur parquet, ont un comportement automobile bien plus prudent que la moyenne, et qu'une réduction de prime apparaîtrait ainsi comme justifiée[94]. Le risque peut dès lors être bien plus subjectivisé, individualisé. C'est, selon François Ewald, le passage de la notion de risque comme événement à celle de risque de comportement : *« les risques [...] étaient d'abord appréhendés par leurs caractéristiques objectives, à partir des événements qui en marquent la réalisation [...] on peut désormais les observer comme caractéristiques du comportement des agents »*. L'**assurance comportementale** concerne déjà les comportements des automobilistes à travers les coefficients de réduction-majoration (plus connus sous le nom de bonus ou malus) fondement du « pay as you drive » (qui se fonde sur les antécédents des conducteurs notamment en termes de vitesse moyenne). Plus encore, l'adaptation du coût des offres selon le style de conduite (accélérations, freinages brusques) est également possible grâce aux capteurs dont certains véhicules sont équipés *(« pay how you drive »)*.

En santé, l'individualisation ne mène pas encore à une segmentation tarifaire explicite, mais le programme Vitality de la société Generali révèle comment un système de récompenses peut indirectement permettre de s'adapter aux comportements des clients. Vitality se présente comme un programme visant à améliorer le bien-être en mettant à disposition *« des recommandations et des outils pour [...] encourager à mener une vie plus saine »* et en récompensant ceux qui atteignent leurs objectifs – plutôt qu'en pénalisant ceux qui ne les atteignent pas – *« grâce à des réductions et des offres avantageuses »* chez des partenaires[95]. *« Likes »* émis sur les réseaux sociaux et données de profil sur Facebook, par exemple, pourraient également servir à proposer des tarifs automobile avantageux.

Qui dit risque individualisé dit possibilité de **services de prévention augmentés** qui vont *« agir directement sur la source du risque pour tenter d'éviter qu'il survienne »* (par des incitations relatives à l'activité physique, la nutrition etc.), comme l'explique Fabrice Faivre (MACIF)[96]. Argument de santé publique en faveur des assurés, l'individualisation annonce aussi des modèles renégociés en assurance, fondés sur la détection des profils à haut risque et sur une nouvelle relation possible des assureurs au client.

La portée de cette personnalisation mérite toutefois d'être nuancée : une segmentation tarifaire trop fine ne serait pas nécessairement dans l'intérêt d'un assureur, du fait des conséquences potentielles qu'impliquerait une erreur en absence de volumes significatifs. Il reste encore à savoir si le cadre légal actuel est adapté à un tel mouvement. Celui-ci tend à restreindre l'utilisation de données par les assureurs au nom de principes tels que la protection des données à caractère personnel (le SNDS créé par la loi de « modernisation de notre système de santé » limite l'accès des assureurs aux données de santé) ou la lutte contre les discriminations. A titre d'exemple, la Cour de justice de l'Union européenne interdit l'utilisation du genre comme variable au sein d'un modèle statistique en assurance au nom du principe d'égalité de traitement entre les hommes et les femmes[97]. Florence Picard (Institut des Actuaires)[98] émet des réserves quant à la pertinence d'écarter un tel critère qui pourrait trouver toute sa place dans certains modèles. Cécile Wendling (AXA)[99] mentionne comment cette obligation du droit européen pourrait toutefois être mise à mal si les algorithmes de *machine learning* venaient à se déployer, inférant ainsi par eux-mêmes les critères permettant d'identifier le genre (couleur d'un véhicule etc.). En somme, l'avenir de ces pratiques semble aujourd'hui dépendre, d'une part, du degré de développement futur des objets connectés et, d'autre part, de la volonté qu'auront les citoyens de transmettre volontairement et consentir à l'utilisation de certaines des données les concernant pour améliorer leur santé par exemple.

Emploi, RH, recrutement

Alors que chômage et conditions de travail sont au centre des préoccupations sociétales, les initiatives convoquant des algorithmes foisonnent pour répondre aux grands enjeux du marché de l'emploi.

Les particuliers, d'une part, peuvent recourir à des **agrégateurs d'offres d'emploi** qui se perfectionnent. L'APEC (Association pour l'emploi des cadres) dispose par exemple d'un algorithme sémantique permettant non seulement de rechercher les offres d'emploi selon des mots-clés, mais également d'induire automatiquement d'un CV le référentiel de compétences et de talents qui permettra de suggérer ensuite les offres d'emploi le plus finement possible[100]. Pôle

93 Evénement organisé par la Ligue des Droits de l'Homme, le 15 septembre 2017.
94 Dominique Cardon, *A quoi rêvent les algorithmes,* Paris, 2015, p.52
95 Site officiel de Vitali.
96 Evénement organisé par la Ligue des Droits de l'Homme, le 15 septembre 2017.
97 CJUE, 1er mars 2011, affaire C-236/09 dite « Test-Achats »
98 Evénement organisé par Fotonower, le 22 septembre 2017.
99 Evénement organisé par la Chaire IoT de l'ESCP Europe, le 20 septembre 2017.
100 Le Directeur des systèmes d'information de l'APEC a présenté cet outil lors de l'événement organisé par FO-Cadres, le 18 avril 2017.

Emploi dispose également de sa propre solution algorithmique d'agrégation des offres d'emploi.
Dans le cadre d'une réflexion éthique, c'est surtout l'appropriation par les entreprises – et notamment les directions des ressources humaines (DRH) – qui interpelle. Sans impliquer une réelle rupture des missions traditionnelles du DRH, l'algorithme faciliterait l'atteinte des objectifs de **recrutement** et de **gestion des ressources humaines,** à savoir : répondre aux attentes de rapidité dans la mobilité et le recrutement, accentuer l'emprise des collaborateurs sur leur propre parcours et, enfin, mettre à la disposition des managers la ressource adéquate pour l'atteinte des objectifs[101]. C'est notamment le coût de la « mauvaise embauche » qui pourrait être évité, voire la réduction à une échelle plus large du chômage. Prédire pour mieux satisfaire collaborateur et manager, en tirant profit d'une masse de données pertinentes : telle est la promesse de l'algorithme.

Recrutement : L'algorithme peut constituer un **instrument de « matching » affinitaire,** basé sur la sémantique, mobilisé par le DRH pour préqualifier le volume parfois conséquent de CV reçus pour une offre d'emploi donnée. Au vu de la durée moyenne très réduite de qualification d'un CV par un humain, nombreux sont ceux qui invoquent la plus grande « rigueur » de l'algorithme. La Harvard Business Review publiait ainsi une étude en 2014 affirmant qu'un algorithme peut surpasser le recruteur humain et éviter des présupposés fréquents chez ce dernier, tels que la tendance à corréler systématiquement prestige d'une université et performance future.
Gestion des RH : L'algorithme pourrait identifier les collaborateurs les plus à même d'être performants dans un rôle déterminé, en allant chercher ceux qui n'auraient pas candidaté à une offre de poste donnée. La mobilité interne serait également optimisée par le ciblage de formations appropriées pour un collaborateur afin d'esquisser pour lui un nouveau cheminement de carrière.
Qualité de vie : D'autres applications, pour lesquelles la réflexion éthique est plus que de rigueur, concernent la compréhension de certains phénomènes sociaux au sein de l'entreprise : analyse des facteurs justifiant l'absentéisme, prédiction des risques psychosociaux, calcul du risque de départ d'une organisation etc.

C'est bien la donnée qui constitue ici le matériau à faire fructifier pour résoudre certains défis du marché de l'emploi, à commencer par l'insuffisance de méthodes traditionnelles de recrutement (CV, entretiens) considérées lacunaires pour « atteindre » l'intimité de l'individu. Aptitudes comportementales et cognitives (« soft skills ») sont désormais plus activement recherchées : l'algorithme capitalise sur la donnée répartie au sein voire à l'extérieur de l'entreprise pour œuvrer en ce sens.

Ce sont d'abord les **données internes** à une organisation qui peuvent alimenter l'algorithme, à condition qu'elles puissent être rassemblées et fiabilisées. Si ces données existent, elles sont *« détenues pour partie par les collaborateurs, pour partie par les fonctions RH et pour partie pour les managers »*[102] et elles s'inscrivent plus dans une *« logique de "rendre compte" que d'exploitation pour des motifs précis »*[103].

Parfois jugées insuffisantes, la collecte de **données externes** (telles que les informations relatives aux parcours professionnels publiées sur les réseaux sociaux) est également attrayante pour de nombreuses organisations.

Les traitements algorithmiques semblent encore aujourd'hui limités[104], les quelques exemples existants aujourd'hui ne recourant pas à l'intelligence artificielle et au *machine learning*. Le frémissement est cependant tangible : le nombre de start-ups ayant pour objet les RH est passé de 200 à 600 en l'espace de deux ans[105]. Il est trop tôt pour évaluer de manière certaine l'impact qu'auront ces technologies sur les pratiques de recrutement et la gestion des talents[106]. N'est-il pas, par exemple, trop ambitieux d'affirmer qu'un algorithme pourrait se substituer à l'homme pour effectuer le travail conséquent qu'implique l'évaluation annuelle des collaborateurs ? En matière de recrutement, l'abandon par Google de son système de tri automatisé des candidatures semble révéler certaines limites de l'algorithme. Le perfectionnement des outils pourrait émaner de nouveaux développements en intelligence artificielle – des algorithmes qui construiraient leurs propres référentiels – ou encore d'un recours grandissant à la robotique (l'analyse de l'expressivité émotionnelle lors d'un entretien de recrutement en constitue une illustration[107]). Ces nouveaux outils pourraient engendrer de nouveaux risques : comment distinguer en RH les décisions simples facilement automatisables des décisions complexes pour lesquelles la dimension « humaine » de la profession devra être préservée ?

101 Analyse de Jean-Cristophe Sciberras, directeur des RH France et directeur des relations sociales corporate chez Solvay, lors de l'événement organisé par la CFE-CGC.
102 Sabine Frantz lors de l'événement de FO-Cadres.
103 Béatrice Ravache lors de l'événement de la CFE-CGC.
104 Le service des « questions sociales et RH » de la CNIL ne recense aujourd'hui aucune demande d'autorisation pour de tels traitements à dimension prédictive et n'est consulté qu'à titre informationnel afin de connaître l'avis de la Commission.
105 Jérémy Lamri, fondateur du LabRH, lors de l'événement de la CFE-CGC.
106 Béatrice Ravache, lors de l'événement de la CFE-CGC, évoque au sujet de la fonction de DRH que *« le savoir n'est plus la mémoire, n'est plus l'organisation des données, ni aller les chercher, c'est encore autre chose qui n'est pas forcément évident pour le RH aujourd'hui ».*
107 Laurence Devillers, événement CFE-CGC.

REMERCIEMENTS

La CNIL adresse ses plus vifs remerciements aux personnes et aux institutions qui ont apporté leur participation à cette réflexion collective.

Les partenaires du débat public

- Académie des technologies
- Agence Française de Développement (AFD)
- Association française de droit du travail et de la sécurité sociale (AFDTSS)
- Association française pour l'intelligence artificielle (AFIA)
- Caisse des dépôts et consignations (CDC)
- Centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN)
- Collège des Bernardins
- Comité consultatif national d'éthique (CCNE)
- Comité d'éthique du CNRS (COMETS)
- Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique (CERNA) d'Allistene
- Communication Publique
- Confédération française de l'encadrement – Confédération générale des cadres (CFE-CGC)
- Conseil départemental du Rhône de l'Ordre des Médecins
- Conseil National des Barreaux (CNB)
- Conseil Supérieur de l'Audiovisuel (CSA)
- Conservatoire National des Arts et Métiers (CNAM)
- Cour administrative d'appel de Lyon
- Cour d'appel de Douai
- École des Hautes Etudes en Sciences Sociales (EHESS)
- École Nationale Supérieure de Cognitique (ENSC)
- ESCP Europe, Chaire IoT
- Etalab
- Faculté de Droit de l'Université Catholique de Lille, Centre de recherche sur les relations entre le risque et le droit
- Faculté de Droit de l'Université Catholique de Lyon
- Familles rurales
- Fédération Française de l'Assurance (FFA)
- FO-Cadres
- Fondation Internet Nouvelle Génération (FING)
- Fotonower
- Génotoul societal
- Groupe VYV (MGEN – ISTYA – Harmonie)
- Hôpital Necker
- INNOvation Ouverte par Ordinateur (INNOOO)
- Institut des Hautes Etudes de Défense Nationale (IHEDN)
- Institut des Systèmes Complexes de Paris Ile-de-France (ISC-PIF)
- Institut Imagine
- Institut Mines-Télécom (IMT), Chaire de recherche Valeurs et Politiques des Informations Personnelles
- Institut National des Hautes études de la Sécurité et de la Justice (INHESJ)
- Institut National des Sciences Appliquées (INSA)
- Laboratoire pour l'Intelligence Collective et Artificielle (LICA)
- Le Club des Juristes
- Ligue de l'Enseignement
- Ligue des Droits de l'Homme (LDH)
- Microsoft
- Ministère de l'éducation nationale, via la direction du numérique pour l'éducation (DNE) et son Numéri'lab
- Ministère de la Culture, via la direction générale des médias et des industries culturelles (DGMIC)
- OpenLaw
- Ordre des avocats de Lille
- Randstad
- Renaissance Numérique
- Sciences Po Lille
- Sciences Po Paris
- Société informatique de France (SIF)
- The Future Society at Harvard Kennedy School, AI Initiative
- Universcience
- Université de Bordeaux
- Université de Lille 2
- Université Fédérale de Toulouse
- Université Paris II
- Visions d'Europe

Les autres contributeurs

- Arbre des connaissances
- Autorité de contrôle prudentiel et de résolution (ACPR)
- Autorité des marchés financiers (AMF)
- Montpellier Méditerranée Métropole et son président, M. Philippe Saurel
- Ville de Montpellier

Les 37 citoyens ayant pris part à la concertation citoyenne organisée à Montpellier le 14 octobre 2017.

Jérôme BERANGER • Nozha BOUJEMAA • Dominique CARDON • Jean-Philippe DESBIOLLES • Paul DUAN • Flora FISCHER • Antoine GARAPON • Roger-François GAUTHIER • Hubert GUILLAUD • Rand HINDI • Jacques LUCAS • Camille PALOQUE-BERGES • Bruno PATINO • Antoinette ROUVROY • Cécile WENDLING

LISTE DES MANIFESTATIONS ORGANISÉES **DANS LE CADRE DU DÉBAT PUBLIC**

De fin mars à début octobre, la CNIL a assuré l'animation et la coordination de 45 événements sur les algorithmes et l'intelligence artificielle. Certaines initiatives ont été imaginées spécifiquement à l'occasion du lancement du débat public, d'autres s'inscrivaient déjà dans les projets d'acteurs – institutions publiques, associations, centres de recherche – déjà préoccupés par ces enjeux.

De nombreux acteurs ont fait le choix d'appréhender les algorithmes dans un secteur spécifique (santé, emploi ou éducation par exemple) alors que d'autres ont abordé l'objet technologique dans sa globalité. Enfin, ce sont autant des ateliers d'experts à public restreint que des manifestations orientées vers l'appropriation du grand public (citoyens, étudiants etc.) qui ont jalonné ce processus.

Plus d'informations sur ces manifestations sont disponibles sur le site de la CNIL.

23/01/2017 — EVÉNEMENT DE LANCEMENT :
TABLES-RONDES « Des algorithmes et des hommes »
et « Loyauté, transparence et pluralité des algorithmes »
> CNIL

23/03/2017
25/03/2017 — **COLLOQUE** « Vers de nouvelles humanités ? »
> Universcience

31/03/2017 — **CONFÉRENCE** « Les algorithmes et le droit »
> Université de Lille II

06/04/2017 — **CONFÉRENCE** « Le choix à l'heure du Big Data »
> Sciences Po Lille et Visions d'Europe

08/04/2017 — **DÉBAT** « The governance of emerging technosciences »
> German American Conference at Harvard University

18/04/2017 — **DÉBAT** « Transatlantic perspectives on: AI in the age of social media;
privacy, security and the future of political campaigning »
> The Future Society at Harvard Kennedy School

18/04/2017 — **TABLES-RONDES** « Big Data, ressources humaines : les algorithmes en débat »
> FO-Cadres

04/05/2017 — **CONFÉRENCE** « Loyauté des décisions algorithmiques »
> Université Toulouse III – Paul Sabatier

16/05/2017 — **DÉBAT** « Le numérique tuera-t-il l'Etat de droit ? »
> Collège des Bernadins

19/05/2017 — **COLLOQUE** « La justice prédictive »
> Cour d'Appel de Douai, Ordre des Avocats de Lille et Faculté de Droit de l'Université Catholique de Lille

02/06/2017 — **ATELIERS** « Loyauté des traitements et décision algorithmiques »
> LabEx Centre International de Mathématiques et Informatique de Toulouse

08/06/2017 **DÉBAT** « Algorithmes en santé : quelle éthique ? »
> Groupe VYV (MGEN – ISTYA – Harmonie)

14/06/2017 **TABLE-RONDE** « Intelligence artificielle : l'éthique, à la croisée des RH et du Big Data »
> Confédération française de l'encadrement – Confédération générale des cadres (CFE-CGC)

16/06/2017 **DÉBAT** « Algorithmes, emploi et éthique »
> Association française de droit du travail et de la sécurité sociale (AFDT)

19/06/2017 **JOURNÉE** « Les algorithmes éthiques, une exigence morale et un avantage concurrentiel »
> CERNA d'Allistene et Société Informatique de France (SIF)

19/06/2017 **COLLOQUE** « Humain, non-humain à l'ère de l'intelligence artificielle »
> Université Paris II

21/06/2017 **COLLOQUE** « Intelligence artificielle : autonomie, délégation et responsabilité »
> Ecole Nationale Supérieure de Cognitique (ENSC)

22/06/2017 **ATELIER** « Ethique des algorithmes : enjeux pour la santé »
> Genotoul (plateforme éthique et bioscience)

22/06/2017 **ATELIER DE CROWDSOURCING** « Intelligence artificielle et droit »
> OpenLaw

22/06/2017 **COLLOQUE** « The many dimensions of data »
23/06/2017 **> Institut Mines-Télécom, Chaire de recherche Valeurs et Politiques des Informations Personnelles**

27/06/2017 **COLLOQUE** « Sécurité et justice, le défi de l'algorithme »
> Institut national des hautes études de la Sécurité et de la Justice (INHESJ)

28/06/2017 **PROCÈS FICTIF ET TABLE-RONDE** « Ethique, algorithmes et justice »
> Faculté de Droit de l'Université Catholique de Lyon et Cour administrative d'appel de Lyon

28/06/2017 **JOURNÉE D'ÉTUDES** « Admission Post-bac, cas d'école des algorithmes publics »
> Fondation Internet Nouvelle Génération (FING) et Etalab

03/07/2017 **JOURNÉE** « Algorithmes et souveraineté numérique »
> CERNA d'Allistene

05/07/2017 **JOURNÉE** « Ethique et intelligence artificielle »
> Comité d'éthique du CNRS (COMETS) et Association française pour l'IA (AFIA)

22/08/2017 **DÉBATS** sur les algorithmes dans le champ de l'éducation.
24/08/2017 **> Ligue de l'Enseignement**

05/09/2017 **MATINÉE-DÉBAT** « Le travail à l'ère des algorithmes : quelle éthique pour l'emploi ? »
> Renaissance Numérique et Randstad

11/09/2017 **COLLOQUE** « Convergences du droit et du numérique »
13/09/2017 **> Université de Bordeaux**

14/09/2017 **JOURNÉE** « Algorithmes et Politiques. Les enjeux éthiques des formes de calcul numérique vus par les sciences sociales »
> Ecole des Hautes Etudes en Sciences Sociales (EHESS) et Institut des Systèmes Complexes Ile-de-France

15/09/2017 **JOURNÉE** sur la recherche en santé dans ses aspects éthiques et réglementaires (données, algorithmes)
> Hôpital Necker et Institut Imagine

15/09/2017 **TABLES-RONDES** « Algorithmes et risques de discriminations dans le secteur de l'assurance »
> Ligue des Droits de l'Homme

20/09/2017 **COLLOQUE** « Enjeux éthiques des algorithmes »
> INNOvation Ouverte par Ordinateur (INNOOO)

20/09/2017 **MATINÉE-DÉBAT** « L'éthique des algorithmes et de l'IA est-elle compatible avec la création de valeur dans l'IoT ? : Internet of Things et/ou Internet of Trust ? »
> ESCP Europe (Chaire IoT)

20/09/2017 **COLLOQUE** « Ethique et numérique »
> Collège des Bernardins

21/09/2017 **DÉBAT** « Opportunities and challenges of advanced machine learning algorithms »
> The John F. Kennedy Jr. Forum at Harvard Kennedy School

21/09/2017 **COLLOQUE** « Lex Robotica (à la frontière de la robotique et du Droit : penser l'humanoïde de 2017) »
> Conservatoire National des Arts et Métiers (CNAM)

22/09/2017 **TABLE-RONDE** « IA et éthique des algorithmes »
> Fotonower

26/09/2017 **COLLOQUE** « Algorithmes prédictifs : quels enjeux éthiques et juridiques ? »
> Centre de recherche de l'école des officiers de la gendarmerie nationale (CREOGN)

28/09/2017 **CONSULTATION** « Quel avenir pour la médecine à l'heure de l'intelligence artificielle ? »
> Conseil départemental du Rhône de l'Ordre des Médecins

29/09/2017 **TABLES-RONDES** « Ethique des algorithmes et du big data »
> Agence française de développement (AFD) et Caisse des dépôts et consignations (CDC)

04/10/2017 **COLLOQUE** « Algorithmes et champ de bataille »
Forum-débat « Vers une Intelligence Artificielle bienveillante ? »
> Institut des hautes études de défense nationale (IHEDN)

06/10/2017 **FORUM-DÉBAT** « Vers une Intelligence Artificielle bienveillante ? »
> Laboratoire d'intelligence collective et artificielle (LICA)

12/10/2017 **TABLE-RONDE** « Droit et intelligence artificielle : quelle(s) responsabilité(s) ? »
> Club des Juristes et Microsoft

14/10/2017 **CONCERTATION CITOYENNE** sur les enjeux éthiques des algorithmes
> CNIL

07/09/2017
31/03/2018 **CONSULTATION PUBLIQUE** sur la gouvernance de l'intelligence artificielle
> The Future Society at Harvard Kennedy School

GLOSSAIRE

Algorithme
Description d'une suite finie et non ambigüe d'étapes ou d'instructions permettant d'obtenir un résultat à partir d'éléments fournis en entrée.

Apprentissage machine (ou apprentissage automatique, *machine learning*)
Branche de l'intelligence artificielle, fondée sur des méthodes d'apprentissage et d'acquisition automatique de nouvelles connaissances par les ordinateurs, qui permet de les faire agir sans qu'ils aient à être explicitement programmés.

Apprentissage machine supervisé
L'algorithme apprend de données d'entrée qualifiées par l'humain et définit ainsi des règles à partir d'exemples qui sont autant de cas validés.

Apprentissage machine non supervisé
L'algorithme apprend à partir de données brutes et élabore sa propre classification qui est libre d'évoluer vers n'importe quel état final lorsqu'un motif ou un élément lui est présenté. Pratique qui nécessite que des instructeurs apprennent à la machine comment apprendre.

Big data
Désigne la conjonction entre, d'une part, d'immenses volumes de données devenus difficilement traitables à l'heure du numérique et, d'autre part, les nouvelles techniques permettant de traiter ces données, voire d'en tirer par le repérage de corrélations des informations inattendues.

Chatbot
Agent conversationnel qui dialogue avec son utilisateur (par exemple, les robots empathiques à disposition de malades, ou les services de conversation automatisés dans la relation au client).

Intelligence artificielle (IA)
Théories et techniques « consistant à faire faire à des machines ce que l'homme ferait moyennant une certaine intelligence » (Marvin Minsky). On distingue IA faible (IA capable de simuler l'intelligence humaine pour une tâche bien déterminée) et IA forte (IA générique et autonome qui pourrait appliquer ses capacités à n'importe quel problème, répliquant en cela une caractéristique forte de l'intelligence humaine, soit une forme de « conscience » de la machine).

Conception & réalisation graphique : LINÉAL - 03 20 41 40 76 / www.lineal.fr

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Commission Nationale de l'Informatique et des Libertés

3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Tél. 01 53 73 22 22
Fax 01 53 73 22 00

www.cnil.fr

et éthique numérique
les algorithmes en débat