PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Lignes directrices sur la protection des données Questions éthiques et juridiques dans la recherche et l'innovation en matière de TIC.

COMPRENDRE LA PROTECTION DES DONNÉES

Bud P. Bruegger (ULD)

Remerciements : L'auteur tient à remercier Jörg Pohle, Harald Zwingelberg, Martin Rost, Iñigo de Miguel Beriain et Josh Bruegger pour leurs conseils, leur contribution et leurs commentaires sur les versions préliminaires.

Ce projet a reçu un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne sous la convention de subvention n° 788039. Ce document ne reflète que le point de vue de l'auteur et l'Agence n'est pas responsable de l'usage qui pourrait être fait des informations qu'il contient.

1 Comprendre la protection des données : le règlement européen en quelques mots

1.1 La protection des données dans la loi

Les lignes qui suivent tentent de fournir une introduction concise aux principes de la protection des données dans une perspective européenne. La protection des données à caractère personnel en Europe est un **droit fondamental**, comme l'indique l'article 8 de la *Charte des droits fondamentaux de l'Union européenne*[1] . Elle a été concrétisée par *le règlement général sur la protection des données* (**RGPD**)[2] .

1.2 Objectif de cette introduction

Le RGPD s'étend sur quelque 99 articles qui, à leur tour, sont généralement divisés en plusieurs paragraphes qui, eux aussi, peuvent contenir plusieurs points. En outre, il existe 173 considérants qui aident à l'interprétation des articles. Sur les onze chapitres du RGPD, les quatre premiers concernent directement toute partie qui souhaite traiter des données à caractère personnel. Sans les considérants, ils couvrent un total de 43 articles qui remplissent 28 pages de texte juridique dans la version PDF officielle[3]. Il n'est donc pas surprenant que de nombreuses personnes qui doivent se conformer au RGPD, mais qui ne sont pas versées dans la lecture et l'interprétation de textes juridiques, trouvent que la courbe d'apprentissage est plutôt raide.

La présente introduction tente d'atténuer cette difficulté. Elle ne se contente pas de donner un aperçu du contenu le plus pertinent, mais tente de présenter le RGPD comme un système unique et cohérent. Elle ne se limite pas à énoncer *les* exigences, mais propose un moyen de comprendre également *la raison d'être de* chaque exigence et la manière dont elle constitue une partie nécessaire de l'ensemble du système. Nous espérons que cette approche n'aidera pas seulement à obtenir une bonne vue d'ensemble, mais qu'elle fournira également un niveau de compréhension plus profond. Elle devrait aider les praticiens lorsqu'ils doivent traduire des exigences abstraites en mesures concrètes ou lorsqu'ils doivent décider à quel niveau les mesures fournissent une protection et des garanties suffisantes.

1.3 Le problème que la protection des données aborde

Afin de présenter le RGPD comme un système, il est supposé que la protection des données concerne un seul problème. De toute évidence, cette hypothèse ne fait pas partie de la loi, et le RGPD n'a pas été systématiquement créé pour résoudre un seul problème énoncé. Le problème de base qui est postulé ici pourrait même ne pas trouver de consensus général. Néanmoins, le problème de base postulé est adapté pour expliquer le RGPD de manière systématique comme un système unique. C'est le seul objectif de ce problème de base dans

[1] La Charte des droits fondamentaux a été ratifiée le 7 décembre 2000.
[2] Le RGPDest entré en vigueur le 25 mai 2018.
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (dernière visite le 7/5/2020)

cette introduction. Il peut exister d'autres problèmes de base et d'autres façons d'expliquer systématiquement le RGPD.

Il n'existe pas de consensus général sur le problème que la protection des données aborde réellement[4] . La thèse d'une "minorité influente"[5] est que la protection des données concerne le pouvoir[6] . La présente introduction adopte cette thèse pour aborder le problème de base. En particulier, le problème de base abordé par la protection des données est donc de limiter le pouvoir que les organisations acquièrent sur les individus en traitant leurs données personnelles[7] . L'expression bien connue "*savoir, c'est pouvoir"* exprime précisément cette idée. En effet, la possession d'informations sur un individu lui confère un pouvoir sur cette personne.

En pratique, le traitement de ces informations personnelles peut influencer le comportement d'une personne en soi (par exemple par des *effets de refroidissement*[8]), peut aider à prédire le comportement d'une personne, peut faciliter la manipulation d'une personne pour qu'elle agisse d'une certaine manière (par exemple par une publicité ciblée), ou peut même, dans des cas extrêmes, permettre de forcer une personne à un certain comportement (par exemple par le chantage). Le scandale des données Facebook-Cambridge Analytica illustre la portée du pouvoir fondé sur les informations personnelles dans la mesure où il peut menacer les valeurs fondamentales de la démocratie. L'utilisation des informations personnelles par les États de surveillance totalitaires pour exercer un pouvoir sur ses citoyens est peut-être l'illustration ultime du problème.

Il a toujours été possible de prendre le pouvoir sur les individus grâce aux informations personnelles. Dans le passé, cependant, les capacités techniques limitées limitaient généralement les personnes ayant accès à ce pouvoir[9] et la quantité d'informations pouvant être réellement collectées et traitées. Avec l'avènement du traitement électronique des données, la situation a radicalement changé. Stocker, trouver, combiner et analyser des données est devenu de plus en plus bon marché et accessible à tous. L'avènement des appareils personnels et des capteurs omniprésents a considérablement augmenté la facilité de collecte des données personnelles. La protection des données est la réponse au risque croissant pour les individus qui découle de cette situation.

De la même manière que la législation sur la protection des données peut être considérée comme un remède au déséquilibre des pouvoirs entre les individus et les organisations dans le contexte du traitement des données, la législation antitrust peut être considérée comme un remède au déséquilibre des pouvoirs sur le marché[10] .

---

[4]Voir les pages 104-105 dans Pohle, Jörg. (2018). Datenschutz und Technikgestaltung : Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, Berlin, Allemagne : Humboldt-Universität zu Berlin, DOI http://dx.doi.org/10.18452/19136, https://edoc.hu-berlin.de/handle/18452/19886 (dernière visite le 11/03/2020), (en allemand).

[5] Communications personnelles avec Jörg Pohle.

[6] Voir par exemple Austin, Lisa M., Enough About Me : Pourquoi la vie privée est une question de pouvoir, pas de consentement (ou de préjudice) (1er janvier 2014). À paraître dans Austin Sarat, ed. A World Without Privacy ? What Can/Should Law Do... Disponible sur SSRN : https://ssrn.com/abstract=2524512.

[7] Notez que le traitement des données personnelles à des fins privées dans un ménage est exclu de la protection des données (voir l'article 2, paragraphe 2, point b) du RGPD).

[8] Un effet paralysant est l'inhibition ou le découragement de l'exercice légitime d'un droit ou d'une liberté en raison du traitement des données, comme la vidéosurveillance.

[9] L'accès était par exemple limité, mais son coût était élevé.

[10]Reiner Rehak, Was schützt eigentlich der Datenschutz, présentation au 35th Chaos Communication Congress (35C3), Leipzig, Allemagne, 28/12/18, diapositive 18, https://mirror.netcologne.de/CCC/congress/2018/slides-pdf/35c3-9733- was_schutzt_eigentlich_der_datenschutz.pdf (dernière visite le 24/04/2020).

1.4 Quelle est la structure de base du RGPD ?

En principe, il n'est pas souhaitable d'acquérir un pouvoir sur les individus par le biais du traitement de leurs données, car cela peut entraver les droits et libertés des individus. Interdire totalement le traitement des données à caractère personnel serait toutefois excessif. En particulier, cela pourrait porter atteinte à d'autres libertés et droits fondamentaux, tels que la liberté d'exercer une activité commerciale[11] . C'est pourquoi la législation sur la protection des données à caractère personnel doit trouver un équilibre entre tous ces droits.

Par conséquent, le RGPD utilise la structure de base suivante :

- Seul le traitement à certains types de **finalités** est autorisé ;
- et seulement sous certaines conditions quant à la manière dont le traitement est **mis en œuvre**.

Ceci est expliqué plus en détail dans la suite.

Dans ce contexte, la **mise en œuvre du traitement** détermine entre autres quelles données sont collectées, quelles ressources humaines et techniques (matériel et infrastructure informatiques) traitent les données et comment (logiciels et procédures) et pendant combien de temps, et à qui les données sont divulguées.

1.5 À quelles fins le traitement est-il autorisé ?

En principe, le RGPD interdit le traitement des données à caractère personnel, sauf s'il est effectué à des **fins légitimes et licites**[12] .

Une **finalité** décrit un objectif concret qui doit être réalisée par le traitement.

Légitime signifie la conformité à la lettre de la loi (sans se limiter au RGPD), à l'esprit de la loi (par exemple, sans exploiter les vides juridiques), aux valeurs de la société (telles qu'exprimées par exemple dans la Charte européenne des droits fondamentaux) et aux principes de l'éthique. Dans certains domaines de recherche, le respect de l'éthique peut être vérifié dans le cadre de procédures formelles telles que l'approbation par un comité d'éthique de la recherche.

La licéité est définie à l'article 6 du RGPD. En particulier, pour que le traitement soit licite, ses finalités doivent relever de l'une des six catégories prévues, appelées *base légale*[13] . Les responsables du traitement ne sont autorisés à traiter des données à caractère personnel que s'ils peuvent présenter une base légale valable.

En ce qui concerne le problème abordé par la protection des données, cela signifie que l'acquisition d'un pouvoir sur les individus n'est alors autorisée que lorsqu'elle sert des objectifs légitimes du type de ceux prévus par le RGPD.

1.6 Quelles sont les conditions de mise en œuvre du traitement ?

Le traitement des données à caractère personnel à des fins légitimes et licites est donc autorisé, mais seulement sous certaines conditions de mise en œuvre. Ces conditions sont décrites plus en détail ci-après.

---

[11] Voir l'article 16 de la Charte européenne des droits fondamentaux.
[12] Voir l'article 5, paragraphe 1, points a) et b), du RGPD.
[13] Voir l'article 6, paragraphe 1, du RGPD.

La raison d'être de ces conditions est de **limiter et d'équilibrer le pouvoir** acquis par l'organisation qui traite les données à caractère personnel (les "***responsables du traitement***") sur les personnes concernées (les "***personnes concernées"***).

Pour résumer, cela se fait de la manière suivante :

- Responsabilité du responsable du traitement,
- la responsabilisation des personnes concernées,
- équilibre des pouvoirs par le biais d'une autorité de contrôle,
- limiter les responsables du traitement à utiliser le pouvoir acquis uniquement pour réaliser les finalités légitimes déclarées,
- la limitation du pouvoir acquis à ce qui est minimalement nécessaire pour réaliser les finalités légitimes,
- la protection des investissements et du patrimoine des personnes concernées,
- l'interdiction du traitement qui n'est pas adapté à la finalité.
- Les différents points sont examinés plus en détail dans la suite du document.

1.6.1 Les responsables du traitement sont entièrement responsables

Une première mesure pour limiter le pouvoir des responsables du traitement consiste à les tenir pleinement responsables de l'ensemble de l'activité de traitement. Il s'agit de l'un des principes clés du RGPD (voir l'art. 5(2)). Il va au-delà du simple fait d'obliger les responsables du traitement à rendre leur traitement **transparent**[14] (pour les personnes concernées et les autorités de contrôle) en obligeant les responsables du traitement à être en mesure de **démontrer** réellement leur **conformité** au RGPD. De toute évidence, cela ouvre le traitement à la surveillance. De plus, cela attribue clairement la "charge de la preuve" : ce ne sont pas les personnes concernées ou les autorités de contrôle qui doivent démontrer une violation du RGPD ; la non-transparence qui cache la non-conformité est en soi une violation.

Pour y parvenir, dans un premier temps, le RGPD veille à ce que l'entière **responsabilité soit** clairement entre les mains du (des) responsable(s) du traitement (conjoint) qui détermine(nt) les finalités et les moyens du traitement[15] . Cela se fait, par exemple, en obligeant les responsables du traitement à exercer un contrôle sur leurs **employés**[16] et en stipulant des contrats[17] avec d'éventuels services informatiques externes (appelés ***sous-traitants***) qui garantissent un contrôle jusqu'au droit d'audit sur place par le responsable du traitement[18] .

Une fois la responsabilité clarifiée, les responsables du traitement sont tenus de faire preuve d'une **transparence** totale concernant le traitement. Ils doivent notamment **informer de** manière proactive **les personnes concernées** de l'existence et des principales caractéristiques du traitement[19] et fournir d'autres types d'informations sur demande[20] . À cette fin, les responsables du traitement doivent généralement aussi désigner un *délégué à la protection des données*[21] dont les coordonnées font partie des informations obligatoires[22] et qui sert de point de contact pour les personnes concernées[23] .

---

[14] Notez que la transparence est également un principe du RGPD, comme le stipule l'art. 5(1)(a).
[15] Voir l'art. 4(7) du RGPD.
[16] Voir l'art. 29 et 32(4) du RGPD.
[17] Voir l'art. 28(3) du RGPD.
[18] Voir l'art. 28(3)(h) du RGPD.
[19]Voir l'art. 13 et 14 du RGPD.
[20] Voir par exemple les art. 15 12(3) et 19 du RGPD.
[21] Voir l'art. 37 du RGPD.

Les responsables du traitement doivent en outre notifier les violations de données à l'**autorité de contrôle** compétente[24] et (si elles sont susceptibles d'être exposées à un risque élevé) aux personnes concernées[25] . En outre, pour les autorités de contrôle, les responsables du traitement doivent tenir des registres de toutes les activités de traitement qui concernent des données à caractère personnel[26] et être en mesure de présenter une *analyse d'impact sur la protection des données* pour les activités de traitement qui sont susceptibles d'entraîner un risque élevé pour les droits et libertés des personnes concernées[27] . Cette dernière est un instrument de choix pour *démontrer la* conformité avec le RGPD.

1.6.2 Renforcement du pouvoir des personnes concernées

Étant donné qu'il existe un déséquilibre de pouvoir dans le traitement des données, le RGPD donne le pouvoir à la partie la plus faible, c'est-à-dire les personnes concernées. Les personnes concernées passent ainsi du statut d'observateurs impuissants du traitement à celui de parties prenantes qui peuvent défendre leurs droits et libertés en intervenant.

Le RGPD habilite les personnes concernées principalement par le biais de ce que l'on appelle les ***droits des personnes concernées***[28] . Il s'agit notamment des droits suivants[29] :

- Le *droit d'accès*[30] aux données relatives aux personnes concernées qui sont traitées,
- le *droit de rectification*[31] qui permet de corriger les données personnelles inexactes et de compléter les données incomplètes,
- le *droit à l'effacement*[32] que l'on appelle aussi le *droit à l'oubli*,
- le *droit à la limitation du traitement*[33] qui permet aux personnes concernées d'exiger la suspension du traitement de leurs données dans certaines circonstances[34] .
- le *droit d'opposition*[35] qui permet aux personnes concernées d'exiger la cessation du traitement de leurs données dans certaines circonstances.
- le *droit de ne pas faire l'objet d'une décision fondée uniquement sur un traitement automatisé* produisant des effets juridiques le concernant ou l'affectant de manière significative de façon similaire[36] qui comprend le *droit d'obtenir une intervention humaine de la part du responsable du traitement*[37] .

Au-delà de ces droits, les personnes concernées disposent également :

---

[22] Voir l'art. 13(1)(b) et 14(1)(b) du RGPD.
[23] Voir l'art. 38(4) du RGPD.
[24] Voir l'art. 33 du RGPD.
[25] Voir l'art. 34 du RGPD.
[26] Voir l'art. 30 du RGPD.
[27] Voir l'art. 35 du RGPD.
[28] Voir le chapitre 3 du RGPD qui comprend les articles 12 à 23.
[29] Notez que le droit à la portabilité des données est abordé dans la section sur la protection du patrimoine de la personne concernée.
[30] Voir l'art. 15 du RGPD.
[31] Voir l'art. 16 du RGPD.
[32] Voir l'art. 17 du RGPD.
[33] Voir l'art. 18 du RGPD.
[34] Ces circonstances sont énumérées à l'art. 18(1) du RGPD.
[35] Voir l'art. 21 du RGPD.
[36] Voir l'art. 22 RGPD.
[37] Voir l'art. 22(3) du RGPD.

- le *droit de retirer le consentement à tout moment*[38] dans le cas où la base légale du traitement est le consentement[39] ,
- le droit d'être informé par le responsable du traitement de la propagation des invocations des droits des personnes concernées à tous les destinataires[40] .

1.6.3 Équilibrer le pouvoir par l'institution d'autorités de contrôle

Bien que les personnes concernées soient habilitées par les droits susmentionnés, leurs ressources peuvent être insuffisantes pour les faire valoir. En particulier, elles peuvent sembler incapables de faire usage de leur *droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant*[41] par elles-mêmes. Pour cette raison, le RGPD accorde aux personnes concernées le ***droit de déposer une plainte auprès d'une autorité de contrôle***[42] .

En d'autres termes, le RGPD fournit aux personnes concernées un allié dont le pouvoir est comparable ou supérieur à celui du responsable du traitement et donc suffisant pour faire valoir les droits des personnes concernées.

Le RGPD confère donc des pouvoirs aux autorités de contrôle[43] . Ces pouvoirs vont des pouvoirs d'investigation [44], tels que les audits sur place[45] , aux pouvoirs de correction [46], tels que l'imposition d'amendes administratives[47] , l'ordre de suspendre les flux de données vers les destinataires[48] , et l'interdiction totale du traitement[49] .

1.6.4 Limiter les responsables du traitement à l'utilisation du pouvoir uniquement pour réaliser les finalités légitimes déclarées.

En démontrant que les finalités sont légitimes et licites, un responsable du traitement a justifié le gain de pouvoir qui accompagne l'activité de traitement. Il est évident que l'utilisation de ce pouvoir pour toute autre finalité ne serait pas justifiée. En d'autres termes, l'autorisation de traiter est limitée aux finalités déclarées pour lesquelles les données sont collectées.

Le RGPD appelle ce principe **"limitation de la finalité"** (voir art. 5(1)(b)).

La manière de mettre en œuvre ce principe sur le plan technique et organisationnel consiste à **séparer** les différentes activités de traitement.

Comme deuxième ligne de défense, même si des données provenant de différentes activités de traitement étaient de toute façon combinées, des mesures telles que la pseudonymisation peuvent rendre plus difficile leur combinaison effective en reliant des enregistrements de données concernant la même personne.

Il convient de noter que cette règle empêche également l'**accumulation de pouvoir** en combinant les données provenant de différentes activités de traitement. Une telle combinaison permettrait généralement d'obtenir un aperçu plus approfondi de la vie des personnes

---

[38] Voir l'art. 7(3) du RGPD.
[39] Voir l'art. 6(1)(a) et 9(2)(a) du RGPD.
[40] Voir l'art. 19 du RGPD, deuxième phrase.
[41] Voir l'art. 79 du RGPD.
[42] Voir l'art. 77 du RGPD.
[43] Voir l'art. 58 du RGPD.
[44] Voir l'art. 58(1) du RGPD.
[45] Voir l'art. 58(1)(b) et (f) du RGPD.
[46] Voir l'art. 58(2) du RGPD.
[47] Voir l'art. 58(2)(i) du RGPD.
[48] Voir l'art. 58(2)(j) du RGPD.
[49] Voir l'art. 58(2)(f) du RGPD.

concernées, couvrant plus d'aspects, ou une couverture plus large des connaissances comprenant un plus grand nombre de personnes concernées. Dans les deux cas, on peut faire valoir que le pouvoir combiné est supérieur à la somme de ses parties.

1.6.5 Minimisation du pouvoir à ce qui est nécessaire pour réaliser les finalités déclarées.

Si la démonstration de la légitimité et de la licéité des finalités a justifié le traitement en tant que tel, celui-ci doit être mis en œuvre de manière à réduire le gain de pouvoir à ce qui est minimalement nécessaire pour réaliser ces finalités. Cette minimisation du pouvoir concerne les trois aspects suivants :

- Contenu informatif des données à caractère personnel,
- le degré d'association des données avec la personne concernée, et
- la limitation des destinaires qui ont accès au pouvoir.

Ceux-ci sont décrits plus en détail dans ce qui suit.

1.6.5.1 Minimisation du contenu de l'information (c'est-à-dire du pouvoir)

Puisque savoir c'est pouvoir, la minimisation du pouvoir signifie que les données personnelles collectées doivent être minimisées. Seules les données dont on peut démontrer qu'elles sont nécessaires pour réaliser les finalités déclarées peuvent être légitimement collectées.

Le RGPD appelle ce principe **"minimisation des données" (**voir art. 5(1)(c)). Plus précisément, il exige que les données collectées soient "adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées". Dans une perspective temporelle, elle exige également que les données ne soient pas conservées plus longtemps que nécessaire aux fins poursuivies. Dans le cas d'un traitement plus complexe comportant plusieurs phases, chaque phase ne doit comporter que les données réellement nécessaires et le contenu des informations doit être réduit entre les phases.

1.6.5.2 Minimiser l'association à la personne concernée

La facilité avec laquelle le pouvoir sur la personne concernée peut être exercé dépend de la mesure dans laquelle la personne concernée peut être associée aux données. La force de l'association entre les données et la personne concernée doit donc être réduite au minimum.

Le RGPD distingue trois types de données avec différents degrés d'association :

- Données identifiantes complètes,
- des données pseudonymisées, et
- des données anonymes.

La première permet l'"identification **directe**"[50] de la personne concernée par l'utilisation d'un "**identifiant"** tel qu'un nom, un numéro d'identification, des données de localisation, [ou] un identifiant en ligne"[51] ; les **données pseudonymisées ne** permettent l'**identification que par l'utilisation d'"informations supplémentaires**"[52] ; et les **données anonymes** lorsque "**la personne concernée n'est pas ou plus identifiable**"[53] .

[50]Ce terme est introduit dans l'art. 4(1) du RGPD.
[51] Ce libellé est extrait de l'art. 4(1) du RGPD.
[52] Notez que ce terme est utilisé dans l'art. 4(5) du RGPD qui fournit la définition de la *pseudonymisation*.
[53] Cette formulation est extraite de la cinquième phrase du considérant 26 du RGPD.

Par analogie avec la minimisation des données, les données doivent être collectées avec le degré minimal d'association avec la personne concernée. En ce qui concerne l'aspect temporel, "les données à caractère personnel sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités"[54] . Dans le cas d'un traitement plus complexe comportant plusieurs phases, chaque phase ne doit comporter que le degré minimal d'association réellement nécessaire et une pseudonymisation ou une anonymisation doit être utilisée entre les phases.

Le RGPD appelle ce principe **"limitation du stockage"** (voir art. 5(1)(e)).

1.6.5.3 Limitation de l'accès au pouvoir

Le pouvoir est entre les mains des personnes et des organisations. Si la connaissance est un pouvoir, ce pouvoir n'est disponible que pour les parties auxquelles les données à caractère personnel sont divulguées. Le RGPD appelle ces parties *des destinataires*[55] . Il peut s'agir d'employés du responsable du traitement ou du sous-traitant, de destinataires tiers prévus ou de parties involontaires telles que des attaquants.

L'accès au pouvoir doit être limité à ce qui est nécessaire pour réaliser les finalités déclarées. Le RGPD appelle ce principe **"confidentialité"**[56] .

La confidentialité comporte deux aspects :

- Empêcher l'accès par des parties non autorisées, et
- restreindre l'accès aux parties autorisées.

Le premier protège dans une large mesure contre les attaquants externes grâce à des mesures telles que le cryptage des données au repos ou des communications et les pare-feu. La seconde est généralement appelée **contrôle d'accès**. Il permet de s'assurer que la partie accédant aux données est bien autorisée (authentification), de limiter l'accès aux données nécessaires (droits d'accès) et éventuellement de restreindre l'accès aux moments où il est nécessaire.

1.6.6 Protection du patrimoine de la personne concernée

Dans de nombreux types d'activités de traitement, les données à caractère personnel stockées par le responsable du traitement ont également une valeur importante pour la personne concernée. Les collections de photos, les suites bureautiques et les systèmes de gestion de documents basés sur l'informatique dématérialisée, mais aussi les données médicales stockées chez le médecin d'un patient, en sont de parfaits exemples. Nous appelons ces données le *patrimoine*.

Ce patrimoine peut avoir une valeur bien moindre pour le responsable du traitement, qui peut être réticent à investir de manière significative dans leur protection. En outre, l'une des façons pour un responsable du traitement d'exercer un pouvoir sur une personne concernée est de subordonner l'accès à son patrimoine à certaines conditions.

Pour empêcher un tel exercice du pouvoir, le RGPD impose aux responsables du traitement de protéger le patrimoine des personnes concernées. En particulier, il exige de protéger ce patrimoine contre :

- la perte, la destruction ou les dommages accidentels[57] , et

---

[54] Ce libellé est extrait de l'art. 5(1)(e) du RGPD.
[55] Voir l'art. 4(9).
[56] Voir l'art. 5(1)(f).

- refus de laisser la personne concernée utiliser le patrimoine indépendamment du responsable du traitement.

Le premier type de protection est également connu sous le nom de **disponibilité** et de **résilience**[58] . La seconde est appelée **portabilité des données** et constitue l'un des droits de la personne concernée[59] .

1.6.7 Interdiction d'un traitement qui n'est pas adapté à sa finalité

L'obtention d'un pouvoir par le biais d'un traitement qui ne permet pas de réaliser les finalités déclarées est évidemment illégitime.

Le RGPD utilise deux principes pour faire respecter l'adéquation à la finalité :

- **L'intégrité** (voir l'art. 5(1)(f)) et
- **La précision** (voir art. 5(1)(d)).

La première impose de protéger les données contre les dommages accidentels et les modifications non autorisées ; la seconde impose que les données soient tenues à jour et exactes et que, lorsque ce n'est pas le cas, les données soient effacées ou rectifiées sans délai.

1.7 La notion de risque

Le *risque* est un concept important dans le RGPD[60] . Le point de vue présenté, selon lequel la protection des données consiste à corriger le déséquilibre des pouvoirs entre le responsable du traitement et la personne concernée, clarifie également la notion de risque :

Le risque principal est que le traitement des données à caractère personnel entraîne effectivement un déséquilibre de pouvoir qui restreint les droits et libertés des personnes concernées. De ce point de vue, il devient clair que le risque n'est pas qu'un événement indésirable se produise (comme une attaque ou une catastrophe naturelle), mais plutôt que le responsable du traitement exerce un pouvoir excessif sur les personnes concernées.

Il convient de noter que cette conception du risque est très différente du risque en matière de cybersécurité. Dans ce domaine, le responsable du traitement est généralement considéré comme le "gentil" qui se défend contre des "attaques" essentiellement externes. En revanche, en matière de protection des données, le comportement du responsable du traitement, c'est-à-dire l'activité de traitement, est la source du risque. La probabilité que cela se produise est de 100 %. Contrairement à la cybersécurité, les responsables du traitement doivent désormais protéger la personne concernée, plus faible, du risque résultant de leur propre traitement. Les responsables du traitement ne sont donc plus automatiquement les bons, mais doivent faire des efforts explicites pour ne pas devenir eux-mêmes des méchants.

Pour les personnes principalement familiarisées avec la cybersécurité, comprendre la protection des données peut nécessiter un changement mental important. Comprendre cette différence est un prérequis pour être en mesure de se conformer au RGPD. Pour une lecture plus approfondie, nous vous recommandons l'article[61] sur les huit différents types de risques.

---

[57] Voir l'art. 5(1)(f) du RGPD.
[58] Voir l'art. 32(1)(b) et (c) du RGPD.
[59] Voir l'art. 20 du RGPD.
[60] Voir par exemple les art. 24(1), 35(1) et les considérants 75 et 84.
[61] Martin Rost, Risques dans le contexte de la protection des données, http://www.maroki.de/pub/privacy/Rost_Martin_2019-02_Risk:_8types_v1.pdf (dernière visite le 8/5/2020).