Le principe de nécessité ou de minimisation des données comme condition à l'innovation responsable : données de qualité, vie privée, cybersécurité et environnement

The principle of necessity or data minimization as a condition for responsible innovation: quality data, privacy, cybersecurity and the environment

Schallum Pierre[1]

[1] Institut intelligence et données (IID), Université Laval, Québec, Canada, schallum.pierre@iid.ulaval.ca

RÉSUMÉ. L'article analyse le principe de minimisation des données ou principe de nécessité énoncé, d'une part, dans le *Règlement général sur la protection des données* (RGPD), en Europe, et, d'autre part, dans la loi 25, au Québec. Il s'appuie respectivement sur Commission nationale informatique et libertés (CNIL), le gendarme français des données personnelles et la Commission d'accès à l'information (CAI), l'organisme québécois de surveillance de l'application de la Loi sur l'accès et de la Loi sur le privé. Il démontre comment le principe de nécessité peut conduire à l'innovation responsable.

ABSTRACT. This article analyzes the principles of data minimization and of necessity outlined in the General Data Protection Regulation (GDPR) in Europe and in Bill 25 in Quebec. It draws respectively on the Commission nationale informatique et libertés (CNIL), the French gendarme of personal data, and the Commission d'accès à l'information (CAI), the overseeing body in Quebec for the application of the Access Act and the Privacy Act. This article demonstrates how the principle of necessity can lead to responsible innovation.

MOTS-CLÉS. Principe de nécessité, Minimisation des données, Innovation responsable, Données de qualité, Vie privée, Cybersécurité, Empreinte carbone et environnement.

KEYWORDS. Principle of necessity, Data minimization, Responsible innovation, Quality data, Privacy, Cybersecurity, Carbon footprint and the environment.

1. Introduction

Qu'il s'agisse d'une collecte, d'une conservation ou d'une utilisation de données personnelles, six principes [EUR 16] doivent être respectés selon le *Règlement général sur la protection des données* (RGPD), ce sont :

- La responsabilité
- La limitation des finalités
- la minimisation des données
- l'exactitude
- la limitation de la conservation
- l'intégrité et la confidentialité.

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

Le présent article porte spécifiquement sur le principe de minimisation des données ou principe de nécessité. Il l'analyse à la lumière du point de vue de la Commission nationale informatique et libertés (CNIL). L'article discute la version québécoise du principe de nécessité énoncé dans la loi 25, en tenant compte de la réflexion de la Commission d'accès à l'information (CAI). Qu'implique ce principe en pratique ? Quel est son impact sur la collecte des données personnelles, dans le contexte des données massives ? Que peut-il pour la vie privée, la cybersécurité, l'environnement et l'innovation ?

2. Du principe de nécessité

Plusieurs législations dans le monde s'appuient sur le principe de minimisation des données ou principe de la nécessité. Le RGPD qui a été adopté en 2018, en Europe, l'emploie, à cinq reprises. Le principe de nécessité désigne le traitement de données personnelles qui sont "adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées" (RGPD, Chapitre II, art. 5). Autrement dit, durant le cycle de vie d'une donnée, de la collecte à la destruction, en passant par la conservation, il importe de limiter les opérations à ce qui est judicieux.

La collecte d'une donnée doit être justifiée et proportionnelle à la finalité d'un projet de recherche ou industriel. Tout projet visant la collecte de données personnelles doit éviter de recueillir des informations qui ne sont pas indispensables ou encore qui restent de l'ordre de l'optionnel. Avant tout recueil de données, il faut clairement déterminer la raison et se limiter à celle-ci respectueusement jusqu'à la fermeture du projet. Le considérant 39 ajoute que les données personnelles ne doivent pas être conservées au-delà de l'atteinte de la finalité. L'entreposage de données personnelles doit s'en tenir au strict minimum. Lorsque la finalité est clarifiée, il devient plus facile de savoir quels types de données collecter et le temps de conservation. La CNIL propose de définir la finalité de la collecte. Voici quelques questions qui pourront conduire à expliciter la finalité :

- "Quel est le but de mon fichier ? (à quoi va-t-il servir ?)
- Est-ce légitime, notamment au regard de mes missions et des droits et libertés des personnes ?
- Comment présenter cette finalité pour la rendre compréhensible par tous ?" [COM 22]

Une fois la finalité déterminée, la CNIL recommande de vérifier la pertinence des données en se posant les questions suivantes :

- "De quelles données ai-je vraiment besoin pour atteindre l'objectif fixé à mon fichier ?
- Ai-je bien distingué les données obligatoires des données facultatives ?
- Les données que je recueille sont-elles objectives ?
- Pourrai-je en toute transparence, donner accès à toute personne qui en fait la demande à l'ensemble des données que je détiens sur elle ?
- Est-ce que je recueille des données sensibles ?
- Ai-je le droit de collecter ces données ?

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

- Est-ce justifié au regard de mes missions ?
- Puis-je faire autrement ?" [CNI 22]

Ces différentes clarifications de la CNIL aident les organisations publiques et privées à considérer la perspective éthique relative aux données personnelles. L'attitude éthique concerne la vigilance sur les données à collecter et leur protection, tout au long de leur construction jusqu'à leur destruction ou anonymisation.

Les références au principe de nécessité se retrouvent aussi dans la loi 25 qui a été adoptée, en 2021, au Québec, quoique l'expression "Principe de minimisation des données" ne soit pas utilisée. La loi 25 précise ceci "La personne qui recueille des renseignements personnels sur autrui ne doit recueillir que les renseignements nécessaires aux fins déterminées avant la collecte." (Loi 25, art. 105.) Le principe de nécessité est primordial. Une collecte ne peut s'effectuer que si, en fonction de ses fins, elle a un "intérêt sérieux et légitime" (art. 104).

Il peut être tout à fait sérieux et légitime c'est-à-dire pertinent qu'une organisation collecte certaines catégories de données personnelles suivant sa mission. Si certains types de données peuvent contribuer à développer ses projets de recherche et développement; répondre à des besoins exprimés par des citoyens et citoyennes; ou permettre l'accès à certains services, une organisation peut procéder à une collecte. Une collecte peut avoir lieu, même sans conservation. C'est le cas, lorsqu'il est nécessaire, pour une organisation, de "visualiser un renseignement personnel, comme ceux contenus sur une pièce d'identité" [CAI 22], d'après la CAI. La collecte est pertinente si, sans les données identifiées, l'organisation ne pourra pas atteindre ses objectifs. Voilà pourquoi, selon la CAI, "en cas de doute, un renseignement personnel est réputé non nécessaire" [CAI 22].

Le critère de nécessité est antérieur au consentement. Un consentement obtenu pour l'utilisation ou la communication d'une donnée personnelle sans le respect du critère de nécessité pourrait être non-valide. Alors que dans certains cas, l'utilisation ou la communication d'une donnée personnelle est possible sans le consentement. Il n'est pas possible d'utiliser ou de communiquer une donnée personnelle sans le critère de nécessité. À titre d'exemple : selon l'article 115 "Une personne qui exploite une entreprise peut, sans le consentement de la personne concernée, communiquer un renseignement personnel à toute personne ou à tout organisme si cette communication est **nécessaire** à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise qu'elle confie à cette personne ou à cet organisme." Les entreprises doivent maîtriser le sens du principe de nécessité afin d'assurer leur mise en conformité à la loi 25, au risque de pénalités très sévères. Comme montrera la prochaine section, l'intérêt d'appliquer le principe de nécessité est qu'il conditionne des données de qualité.

2.1. *Des données de qualité*

Le principe de nécessité signifie que la conservation et l'utilisation d'une donnée personnelle est possible si et seulement cela est incontournable à la finalité préalablement énoncée. Il impose la collecte de données personnelles conformément à l'objectif fixé à l'avance. En d'autres termes, le principe de nécessité exige que l'on se demande pourquoi je veux collecter cette donnée personnelle. S'il n'y a aucune raison, la collecte ne doit pas avoir lieu. Lorsque la raison est énoncée, elle détermine la limite de l'action du recueil de la donnée. Une donnée personnelle qui a été collectée dans un but précis doit être détruite dès que l'objectif aura été atteint.

Il est d'autant plus important d'effacer une donnée obsolète du point de vue de la finalité de la collecte qu'on sait que pour être de qualité une donnée doit être toujours mise à jour. L'adéquation entre la visée du processus et la limitation de la collecte au strict minimum garantit la qualité de la

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

donnée, caractérisée par sa fiabilité, sa précision et son exactitude. En ce sens, moins de données c'est mieux. Gerd Gigerenzer [JOS 22] va jusqu'à soutenir que dans certaines situations moins de données mènent à de meilleures décisions. Un exemple relevant de la discrimination statistique [FEL 22] est l'utilisation de certaines données personnelles non nécessaires comme le sexe ou l'origine qui peuvent rendre les prédictions moins précises.

Le principe de nécessité pourrait jouer un rôle déterminant dans le développement de l'IA. Alors que les géants du web misent sur l'acquisition toujours plus de données massives collectées dans des contextes souvent nébuleux, d'autres écoles de pensée basées sur la frugalité commencent à émerger. Andrew Ng est l'un de ceux qui met l'accent non sur les données massives mais sur la qualité de la donnée. Il décrit l'IA centrée sur les données de qualité comme "the discipline of systematically engineering the data **needed** to build a successful AI system." [SAR 22] Si le principe de nécessité s'applique, la valeur de l'IA augmentera. Cela exige une donnée qui est contextualisée en fonction de sa finalité et dotée d'un processus cohérent en référence à celle–ci. Une donnée collectée et préparée pour l'analyse sans objectif précis n'a pas grand intérêt dans un domaine comme l'apprentissage automatique. Mieux vaut avoir peu de données, nécessaires, mais qui sont de qualité. Une autre dimension du principe de nécessité est son impact sur la protection de la vie privée.

2.2. *De la vie privée*

Protéger la vie privée est l'objectif principal du principe de nécessité. En référence au fameux article "The Right to Privacy" [SAM 90], l'International association of privacy professionals (IAPP) définit la vie privée comme "le droit de ne pas être dérangé, ou l'absence d'interférence ou d'intrusion" [IAP 22]. L'interférence ou l'intrusion est une forme de pouvoir qu'un attaquant peut exercer sur les données personnelles de sa victime. La capacité ou non à contrôler son système d'information lié à des données de qualité est un indicateur d'envergure de l'autonomie d'un pays ou de sa souveraineté.

Le partage d'informations personnelles sur les médias sociaux constitue une source importante pouvant faciliter des interférences. Chaque utilisateur et utilisatrice devrait se demander si tel ou tel renseignement personnel est nécessaire à partager, en sachant l'usage qui pourrait en être fait. Le principe de nécessité peut contribuer à préserver la vie privée car moins les données personnelles sont partagées ou collectées, moins on s'expose à des risques d'incident de confidentialité. Le principe de nécessité s'applique aussi à l'utilisation - primaire ou secondaire - des données personnelles.

Selon l'article 118 de la loi 25, au Québec, la communication de données personnelles est possible, sans consentement, lorsque leur utilisation vise des études, des recherches ou la production de statistiques. Cependant, "La communication peut s'effectuer si une évaluation des facteurs relatifs à la vie privée conclut que : 1° l'objectif de l'étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées; 2° il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées; 3° l'objectif de l'étude, de la recherche ou de la production de statistiques l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées; 4° les renseignements personnels sont utilisés de manière à en assurer la confidentialité; 5° seuls les renseignements **nécessaires** sont communiqués."

Alors que le consentement peut ne pas être demandé, le principe de nécessité doit être respecté. Cela démontre son rôle majeur dans le domaine de la protection des données personnelles. Afin d'aider les professionnelles et professionnels de plusieurs domaines comme la santé qui doivent collecter, conserver et communiquer des données sensibles, des protocoles de communication renforçant la protection de la vie privée ont été créés. L'article "Data minimisation in

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

communication protocols: a formal analysis framework and application to identity management" [MEI 14] présente un cadre visant à comparer les protocoles de communication quant à la confidentialité par la minimisation des données qui concerne aussi la cybersécurité.

2.3. *De la cybersécurité*

Le principe de nécessité est l'un des pivots de la cybersécurité. Selon la norme ISO 27001 [ISO 01], les caractéristiques de la sécurité se déclinent sous trois formes :

- Confidentialité
    - Limiter l'accès et de la divulgation des informations aux personnes autorisées
- Intégrité
    - S'assurer de la fiabilité des données, en évitant qu'elles soient modifiées ou supprimées volontairement ou accidentellement
- Disponibilité
    - Assurer des services 24h/24 et 7j/7 et la résilience du système face à des cyberattaques.

Le défi de collecter moins de données aujourd'hui peut sembler aller à l'encontre des tendances des géants du web. Pourtant, c'est le choix auquel il importe de penser en vue de mieux se protéger [GRO 17]. Une stratégie de minimisation des données pourrait être de collecter le moins de texte possible, en ayant recours par exemple à des cases à cocher [MOH 21]. Une base de données limitée aura un intérêt réduit auprès des milieux cybercriminels. Les mesures gouvernementales peuvent aussi participer à la sécurisation des informations sur les sites web, comme c'est le cas du filtre anti-arnaque et du cyberscore [BER 22], deux grands chantiers que prévoit la France pour 2023. L'impact sur l'environnement constitue un atout du principe de nécessité pour le développement responsable de la technologie.

2.4. *De l'environnement*

L'impact de l'activité humaine sur la planète est un sujet d'actualité. Les usages numériques y jouent un rôle non négligeable évalués de "3 à 4 % des émissions de gaz à effet de serre (GES)" [ARC 22]. L'agence Science.Press [VAL 22] précise que les équipements des utilisateurs émettent entre 37 et 57% de GES; les centres de données, entre 18 et 41%; et le réseau, entre 22 et 35% (voir la figure reprise par l'article de Science Presse)

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

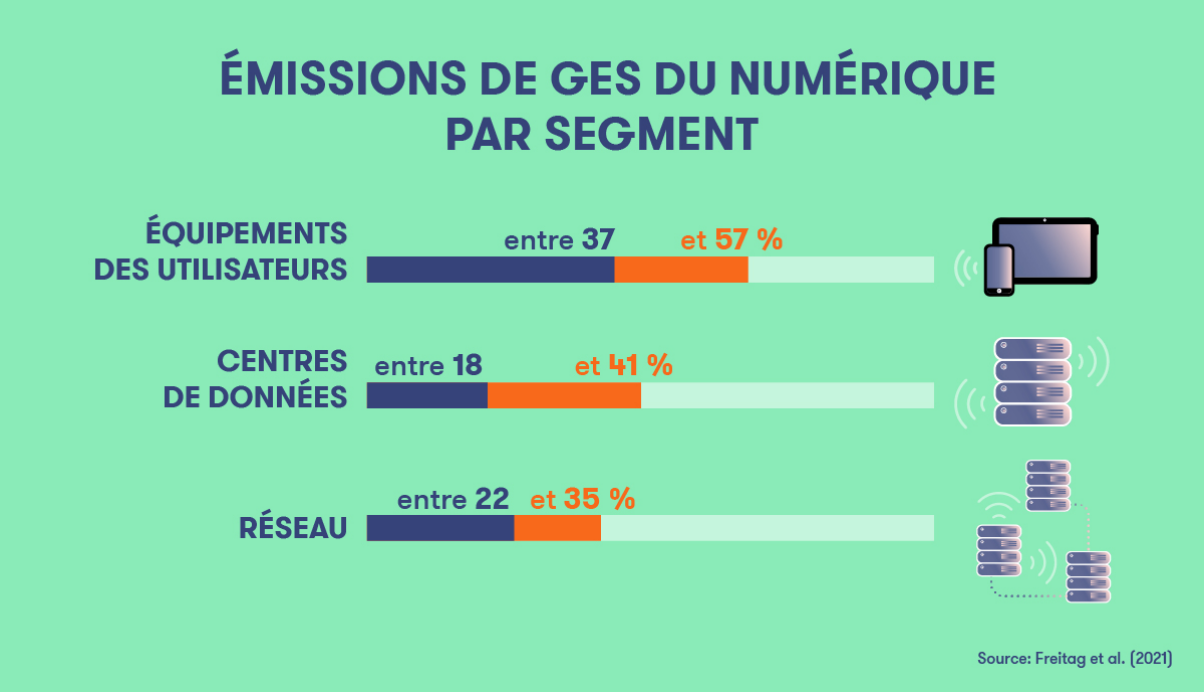

Figure 1. *Tirée de l'Agence-Presse [VAL 22] sur les trois segments d'émission de GES.*

La consommation importante des équipements est en grande partie due à la source énergétique comme le charbon utilisée par les pays producteurs d'équipements comme la Chine. La conservation des données, estimée à "53% des consommations énergétiques" [RÉG 21], exige des infrastructures physiques qui doivent être alimentées en électricité. Les données personnelles voire sensibles qui sont conservées doivent être protégées. L'une des solutions de protection est le chiffrement. Or, cette technique de protection des données, qui est recommandée par la CNIL et valorisée par le secteur de la chaîne de blocs, se révèle très énergivore [RÉG 21]. De même, l'utilisation de certains langages comme Python [RUI 21], très courants en apprentissage automatique pour la cybersécurité, posent aussi des problèmes de consommations d'énergie. Face à ce constat, la mise en œuvre du principe de nécessité peut être une stratégie pour contribuer à la réduction de son empreinte carbone. Une seconde stratégie est le choix de centres de données situés dans des territoires dont l'origine de l'électricité est l'énergie renouvelable. En effet, il y a principalement trois sources [HYD 22] de production de l'électricité dans le monde :

- Les énergies fossiles, 64 %
- Les énergies renouvelables, 25%
- Les centrales nucléaires, 10 %.

Plusieurs régions ou pays du monde comme le Québec ou la Norvège misent sur l'énergie verte et constituent des endroits à faible émission de carbone. Le principe de nécessité mène à la création de l'innovation responsable.

3. De l'innovation responsable

René von Schomberg définit l'innovation responsable comme « [un] processus transparent et interactif par lequel les acteurs sociaux, les chercheurs et les innovateurs collaborent pour l'acceptabilité éthique, la durabilité et la pertinence sociétale (societal desirability) de l'innovation – permettant ainsi l'insertion des avancées des sciences et des techniques dans la société » [RÉM 11]. Dans le secteur de la science des données et plus particulièrement en intelligence artificielle (IA), le principe de nécessité est d'un grand intérêt, si l'on veut mettre en valeur l'innovation responsable.

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

Limiter la collecte au strict minimum peut être un premier pas vers la confiance. Lorsque les citoyens et citoyennes savent que des mesures sont prises pour que leurs données personnelles ne soient pas conservées indéfiniment, dans un contexte de sécurité, cela ne peut qu'améliorer l'acceptabilité sociale. Suivant le principe de nécessité, il incombe aux personnes qui auront à collecter des données personnelles de définir les fins de la collecte. Cette dimension éthique est fondamentale car elle accorde une place au jugement des personnes qui auront à prendre entre autres la décision de limiter le recueil des renseignements personnels et de les effacer dans les délais fixés. L'éthique [AMA 22] doit anticiper l'impact de l'usage des données sur

- L'individu en lien à la protection de la vie privée
- La société en lien à la cybersécurité
- L'environnement en lien à la transition écologique.

Dorénavant, les universités qui préparent certains membres des futures parties prenantes des innovations (intelligence artificielle, administration, droit, éthique, etc…) devront ajouter ces trois impacts dans leur curriculum afin de prendre position pour les générations présentes et à venir. Cette responsabilité face à la durabilité est une culture à intégrer autant dans les milieux de la recherche et de l'enseignement que dans les organisations publiques et privées. Plusieurs universités canadiennes se démarquent dans l'engagement social et environnemental comme montre le récent classement de Quacquarelli Symonds [QUA 22] (voir figure 2)

↑ Overall Rank	University	Environmental Impact Rank	Social Impact Rank
1	University of California, Berkeley (UCB) Berkeley, United States	1	1
2	University of Toronto Toronto, Canada	3	7
3	University of British Columbia Vancouver, Canada	4	2
4	The University of Edinburgh Edinburgh, United Kingdom	10	3
=5	The University of New South Wales (UNSW Sydney) Sydney, Australia	8	=11
=5	The University of Sydney Sydney, Australia	11	5
7	The University of Tokyo Tokyo, Japan	2	=97
8	University of Pennsylvania Philadelphia, United States	15	18
9	Yale University New Haven, United States	6	=11
10	The University of Auckland Auckland, New Zealand	5	=43

Figure 2. *Tirée de Quacquarelli Symonds [QUA 22] sur le classement de l'engagement social et environnemental des universités dans le monde.*

En France, il y a eu, en 2022, un sursaut citoyen auprès des étudiants et étudiantes des Grandes écoles comme AgroParisTech, HEC, Polytechnique et Sciences Po. Ces élèves appellent à mettre fin

à l'inaction. "*"Même si nous, polytechniciens, sommes bercés dans une foi en la rationalité en la science et la technique, nous voyons bien qu'il n'y aura pas de solution miracle, que la technologie ne va pas nous sauver*"" MAR 22].

Dans cette perspective, que peut le principe de nécessité ? Comme condition de l'innovation responsable, il rend possible l'accès à des données de qualité, la protection de la vie privée, la sécurité des données et un engagement environnemental.

4. Conclusion

Le principe de nécessité est l'un des meilleurs moyens par lequel la protection de la vie privée peut être assurée. Il y va de la responsabilité de chaque personne de veiller, par exemple, à son usage des médias sociaux, de ne pas partager ou d'exprimer des informations non-nécessaires. La collecte, le partage et l'utilisation des données personnelles constituent un important défi pour les entreprises qui devront repenser éthiquement leur modèle d'affaires et l'orienter vers la frugalité et la sobriété.

En plus du principe de nécessité, le consentement doit être obtenu afin d'informer le public de l'objectif d'une collecte. En ce sens, sans le consentement de la personne concernée, la pratique de l'inférence [YOU 19] devient questionnable et devrait même être interdite. Le principe de nécessité peut être un véritable allié dans le processus de l'accès à la souveraineté numérique. Moins les données sensibles sont partagées sur les plateformes, plus il sera possible de réduire le risque des cyberattaques. Selon une étude récente menée par Thalès, en 2019, pas moins de 49 % des cyberattaques [MAT 22] sont commanditées par des États. Chaque État doit être conscient de l'impact que peut avoir l'application ou pas du principe de nécessité par les personnes citoyennes et les organisations privées ou publiques concernées.

Bibliographie

[AMA 22] Amandine Lepoutre, "Mathias Vicherat (Sciences Po) : "Nous devons enseigner l'impact, c'est une question d'éthique"", *Challenges*, 4 novembre 2022. https://www.challenges.fr/green-economie/mathias-vicherat-sciences-po-nous-devons-enseigner-l-impact-c-est-une-question-d-ethique_834010#Echobox=1667562571 consulté le 6 novembre 2022.

[ARC 22] ARCEP, *L'empreinte environnementale du numérique*, 26 septembre 2022. https://www.arcep.fr/la-regulation/grands-dossiers-thematiques-transverses/lempreinte-environnementale-du-numerique.html consulté le 10 novembre 2022.

[BER 22] Bercy Numérique, *Cybersécurité : le gouvernement mise sur un filtre anti-arnaque et un cyberscore dès 2023*, 8 novembre 2022. https://www.bercynumerique.finances.gouv.fr/cybersecurite-le-gouvernement-mise-sur-un-filtre-anti-arnaque-et-un-cyberscore-des-2023#:~:text=Imprimer%20la%20page-,Cybers%C3%A9curit%C3%A9%20%3A%20le%20gouvernement%20mise%20sur%20un%20filtre%20anti%2Darnaque,et%20un%20cyberscore%20d%C3%A8s%202023&text=Dans%20le%20cadre%20du%20plan,Fran%C3%A7ais%20des%20attaques%20en%20ligne consulté le 10 novembre 2022.

[CAI 22] CAI, *Protection des renseignements personnels*, 20 septembre 22. https://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1/, consulté le 6 novembre 2022.

[CNI 22] CNIL, *Vérifier la pertinence des données*, https://www.cnil.fr/fr/verifier-la-pertinence-des-donnees consulté le 6 novembre 2022.

[COM 22] Commission nationale informatique et libertés (CNIL), *Définir une finalité*, https://www.cnil.fr/fr/definir-une-finalite, consulté le 6 novembre 2022.

[EUR 16] EUR-Lex, "Règlement général sur la protection des données", *Journal officiel de l'Union européenne*, 27 avril 2016, p. 35-36. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679 consulté le 5 novembre 2022.

[FEL 22] Felipe A. Csaszar, Diana Jue-Rajasingh, Michael Jensen (2022) When Less Is More: How Statistical Discrimination Can Decrease Predictive Accuracy. Organization Science 0(0).

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr

https://doi.org/10.1287/orsc.2022.1626

[GRO 17] Groupe des Nations Unies pour le développement (GNUD), *Confidentialité, éthique et protection des données : Note d'orientation du GNUD concernant les mégadonnées à l'appui de la réalisation du Programme 2030*, 2017. https://unsdg.un.org/sites/default/files/UNDG_French_BigData_final.pdf consulté le 10 novembre 2022.

[HYD 22] Hydro Québec, *Diminuer la pollution numérique, c'est possible*, 2022. https://www.hydroquebec.com/a/decarboner.html, consulté le 10 novembre 2022.

[IAP 22] IAPP, *What does privacy mean?*, 2022. https://iapp.org/about/what-is-privacy/ consulté le 10 novembre 2022.

[ISO 01] ISO/IEC 27001, *Management de la sécurité de l'information*, https://www.iso.org/fr/isoiec-27001-information-security.html consulté le 10 novembre 2022.

[JOS 22] Josh Zumbrun, "When It Comes to Data, Sometimes Less Is More", *The wall street journal*, 4 novembre 2022. https://www.wsj.com/articles/when-it-comes-to-data-sometimes-less-is-more-11667554203 consulté le 8 novembre 2022.

[MAR 22] Martin RICHER, « Les jeunes diplômés et l'entreprise : lost in transition », *Management & RSE*, 11 juillet 2022. https://management-rse.com/les-jeunes-diplomes-et-lentreprise-lost-in-transition/, consulté le 11 novembre 2022.

[MAT 22] Matthieu Bourgeois, *Souveraineté numérique essai pour une reconquête*, préface Guillaume Poupard, Le Cercle de la Donnée et l'Agora41, 2022. p. 67. https://www.lecercledeladonnee.org/wp-content/uploads/2022/01/SOUVENUM_CMJN_Rogne.pdf consulté le 10 novembre 2022.

[MEI 14] Meilof Veeningen, Benne de Weger and Nicola Zannone. "Data minimisation in communication protocols: a formal analysis framework and application to identity management." *International Journal of Information Security* 13 (2014): 529-569. DOI 10.1007/s10207-014-0235-z

[MOH 21] Mohammed Khan, *Data Minimization—A Practical Approach*, 29 mars 2021. https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-a-practical-approach consulté le 10 novembre 2022.

[QUA 22] Quacquarelli Symonds, *QS World University Rankings: Sustainability 2023*, https://www.topuniversities.com/university-rankings/sustainability-rankings/2023 consulté le 6 novembre 2022.

[RÉG 21] Régis Chatellier, *Données et environnement : comment prévenir les marées noires du XXIe siècle ?*, *Laboratoire d'innovation numérique de la CNIL (LINC)*, 19 mai 2021 https://linc.cnil.fr/fr/donnees-et-environnement-comment-prevenir-les-marees-noires-du-xxie-siecle consulté le 10 novembre 2022.

[RÉM 11] Rémi Barré, « Des concepts à la pratique de l'innovation responsable : à propos d'un séminaire franco-britannique », *Natures Sciences Sociétés*, vol. 19, no. 4, 2011, pp. 405-409.

[RUI 21] Rui Pereira, Marco Couto, Francisco Ribeiro, Rui Rua, Jácome Cunha, João Paulo Fernandes, João Saraiva, "Ranking programming languages by energy efficiency", *Science of Computer Programming*, Volume 205, 2021, 102609, ISSN 0167-6423, https://doi.org/10.1016/j.scico.2021.102609

[SAM 90] Samuel D. Warren; Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 195. http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C, consulté le 10 novembre 2022.

[SAR 22] Sara Brown, "Why it's time for 'data-centric artificial intelligence'", *MIT Sloan School of Management*, 7 juin 2022.

https://mitsloan.mit.edu/ideas-made-to-matter/why-its-time-data-centric-artificial-intelligence consulté le 8 novembre 2022.

[VAL 22] Valérie Levée, *Consommation numérique et GES : la fabrication pire que l'utilisation?*, 1er février 2022. https://www.sciencepresse.qc.ca/actualite/detecteur-rumeurs/2022/02/01/consommation-numerique-ges-fabrication-pire-utilisation, consulté le 10 novembre 2022.

[YOU 19] Youyang Qu, Mohammad Reza Nosouhi, Lei Cui, Shui Yu, Chapter 6 - Privacy Preservation in Smart Cities, Editor(s): Danda B. Rawat, Kayhan Zrar Ghafoor, Smart Cities Cybersecurity and Privacy, Elsevier, 2019, Pages 75-88, ISBN 9780128150320, https://doi.org/10.1016/B978-0-12-815032-0.00006-8

© 2022 ISTE OpenScience – Published by ISTE Ltd. London, UK – openscience.fr