CAHIERS IP
INNOVATION & PROSPECTIVE
N°08

Scènes de la vie numérique

Des situations problématiques aux chemins du droit, une exploration du rapport quotidien à la protection des données et de la vie privée.

LINC
CNIL.

ÉDITO

Depuis 2018, la CNIL constate un « effet RGPD » : lorsqu'on explicite mieux leurs droits aux personnes, elles savent s'en saisir. La première année d'entrée en application du règlement, les plaintes reçues ont augmenté de 33 %, puis de 27 % supplémentaires en 2019 avant de se stabiliser autour de 14 000 plaintes en 2020. Selon nos dernières études, 87 % des Français se déclarent aujourd'hui sensibles à l'enjeu de protection des données et 68 % disent connaître la CNIL.

Cette prise de conscience collective s'inscrit donc dans la durée et elle constitue un enjeu stratégique majeur pour la CNIL, qui doit s'organiser pour continuer à répondre efficacement aux demandes des citoyens. Les approches qualitatives, sociologiques et prospectives, mobilisées par son laboratoire d'innovation se révèlent essentielles pour comprendre au mieux les processus et les situations dans lesquels les citoyens sont amenés à contacter la CNIL, et *in fine*, lui permettre de renforcer sa présence dans le quotidien numérique des Français.

Le droit actuel est lui-même le résultat d'une construction socio-historique qui attribue une place centrale aux individus et au principe d'autodétermination informationnelle, selon lequel ces derniers doivent être en mesure de contrôler les informations les concernant, d'être informés, de consentir ou de s'opposer à l'usage par autrui de leurs informations personnelles.

Si la protection des données repose sur un socle juridique commun à tous, elle est appréhendée différemment selon les valeurs individuelles, les cercles sociaux auxquels nous appartenons, les situations rencontrées, les ressources dont on dispose et les contraintes qui s'imposent à nous. Les rapports de pouvoirs et les effets de structures socio-économiques peuvent également entraver les capacités effectives des individus à maîtriser les flux d'informations les concernant.

La protection des données gagne ainsi à être considérée du point de vue de la pluralité des publics et doit être interrogée en tenant compte des inégalités et hiérarchies sociales. Depuis cette perspective, il peut être souhaitable de porter une attention et un message différents selon les vulnérabilités particulières des personnes ou groupes sociaux.

Ce cahier IP procède d'une méthodologie innovante d'analyse sociologique des courriers et des plaintes reçus. Ces études se poursuivront pour affiner la connaissance des publics de la CNIL et leurs pratiques, car si la protection des données résulte d'un droit fondamental attaché à l'individu, elle s'appréhende *collectivement* dans une société démocratique. La CNIL fait le vœu que la série de recommandations présentées en conclusion puisse y parvenir.

Marie-Laure Denis
Présidente de la CNIL

SOMMAIRE

AVRIL 2021
Directeur de la publication :
Louis Dutheillet de Lamothe
et Gwendal Le Grand
Rédacteur en chef :
Bertrand Pailhès
Rédacteurs de ce cahier :
Antoine Courmont, Martin Biéri,
Régis Chatellier, avec l'aide
de Pauline Faget, Stéphanie Chapelle
et Ahlam Ammi.

Conception graphique :
Agence Linéal
03 20 41 40 76
Impression : DILA
04 71 48 51 05
ISSN : 2263-8881 /
Dépôt légal : à publication

La CNIL remercie vivement l'ensemble des membres du Comité de la prospective et les experts extérieurs interviewés ou qui ont participé aux ateliers.

La construction historique des notions de vie privée et de protection des données personnelles

« À Rome, l'on ne trouve guère que les débris des monuments publics, et ces monuments ne retracent que l'histoire politique des siècles écoulés ; mais à Pompéi c'est la vie privée des anciens qui s'offre à vous telle qu'elle était. »

Madame de Staël, Corinne ou l'Italie (1807)

La construction historique des notions de vie privée et de protection des données personnelles

Le droit actuel de la protection de la vie privée et des données personnelles est le résultat d'une construction socio-historique ayant émergé dans le monde occidental, en Europe et aux États-Unis, qui s'inscrit dans le prolongement du « paradigme de la vie privée[1] ». Élaborés dans des contextes nationaux et des traditions juridiques différentes, ces droits présentent comme point commun la place centrale attribuée aux droits de l'individu et au principe d'autodétermination informationnelle.

1 Colin J. Bennett and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, MIT Press, 2003

L'ÉMERGENCE D'UN DROIT À LA VIE PRIVÉE : FONDEMENT DES SOCIÉTÉS MODERNES

Gustav Wentzel, Public domain, via Wikimedia Commons

Les historiens situent l'émergence du concept de vie privée autour du XVIII[e] siècle avec l'apparition d'activités spécifiques qui s'autonomisent progressivement des activités publiques. Auparavant, la confusion est importante entre le public et le privé, catégories qui n'existent pas véritablement[2]. Dans les sociétés traditionnelles, les individus sont enchâssés dans des relations communautaires, il n'y a pas à proprement parler de vie privée, même si des espaces d'intimité existent.

> *« [La notion de vie privée a été] culturellement et historiquement construite comme une valeur sociale appréciée et recherchée et a été inscrite au rang des droits humains fondamentaux, dans un mouvement complexe centré sur un domaine privé incarné d'abord par la famille, puis par l'espace individuel . »*[3]
>
> *Bénédicte Rey, 2012*

La distinction entre le public et le privé émerge à l'Époque moderne. La tradition politique libérale s'est basée sur la distinction nette entre ces deux sphères apparue au sein de la bourgeoisie urbaine des grandes villes européennes des XVI[e] et XVII[e] siècles. Habermas analyse la naissance de l'espace public comme le fruit des Lumières, au travers de l'idéal-type de la « sphère publique bourgeoise », espace de libre délibération et d'argumentation rationnelle. Cette approche se matérialise par des lieux, des salons, des cafés, des clubs et autres sociétés où des individus – les bourgeois cultivés – se rencontrent pour discuter des œuvres de l'esprit de l'époque. Elle est indissociable des démocraties libérales modernes. Cette vision élitiste est toutefois mesurée par Arlette Farge, pour qui l'espace public français du XVII[e] siècle n'était pas limité à l'élite bourgeoise cultivée mais aussi composé des masses populaires[4], et ne prend pas en compte les activités collectives et communautaires publiques, sans être les lieux du débat public, comme les fêtes, les réunions de village, etc.

2 Philippe Ariès, *Histoire de la vie privée*, Seuil, 1985
3 Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012
4 Arlette Farges, *Dire et mal dire, l'opinion publique au XVIII[e] siècle*, Seuil, 1992

En contrepoint, ces espaces publics supposent l'existence de lieux privés, intimes et personnels. Le privé se définit alors par opposition à l'État, et s'entend comme ce qui y échappe[5]. Dans cette même logique, le « cabinet noir », c'est-à-dire la violation de la confidentialité des correspondances par les services de renseignement, qui s'est développé parallèlement à l'essor de la poste à partir du XVII[e] siècle, est l'objet d'une forte opposition au cours du XIX[e] siècle. En s'articulant ainsi avec l'espace public soumis au regard des tiers et au contrôle des autorités, la vie privée est entendue comme le sanctuaire des libertés. S'il ne concerne initialement que certains milieux sociaux et urbains, ce repli sur le privé se généralise peu à peu au cours de ce siècle.

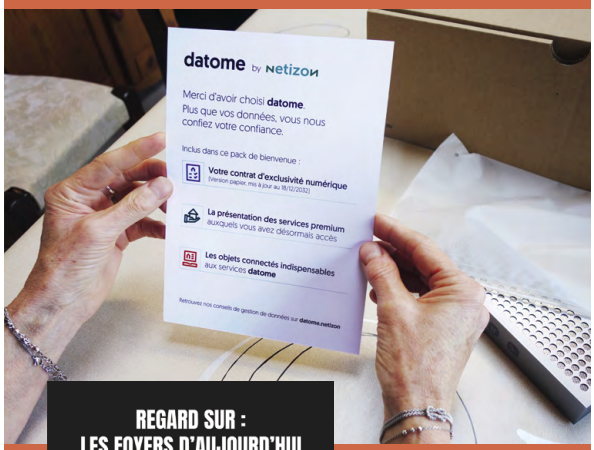
Le premier espace du privé est alors celui de la famille, *« un lieu de refuge où l'on échappe aux regards du dehors, un lieu d'affectivité où s'établissent des rapports de sentiment entre le couple et les enfants[6] »*. Elle devient progressivement un groupe spécifique, distinct du voisinage et de la parenté élargie, ce qui rend possible l'émergence d'une forme d'intimité familiale. Cette association étroite entre famille et vie privée se matérialise dans l'habitat. *« La maison est un lieu-clé pour distinguer le public et le privé. […] une frontière séparant certains types d'activités ou d'informations. […] Ce n'est qu'un des aspects du processus plus large de construction de la notion de vie privée, mais c'est un aspect vital[7] »*.

Puis, se construit peu à peu une sphère d'intimité personnelle qui se distingue de l'intimité familiale, avec notamment la séparation entre une chambre conjugale et une chambre destinée aux enfants. Ce nouvel aménagement de l'espace domestique permet de s'affranchir du regard constant des proches et de construire *« un privé personnel au sein du privé familial »*[8]. La tendance à la spécialisation des pièces reste toutefois dans les faits un privilège de classe supérieure jusqu'au début des années 1960 et l'agrandissement des logements, qui fait apparaître *« une grande nouveauté, pour le peuple du moins : le droit de chaque membre de la famille à sa propre vie privée. La vie privée se dédouble ainsi : au sein de la vie privée familiale, voici celle des individus[9] »*.

FUTUR SPÉCULATIF

Home Sour Home

Dans le scénario *Home Sour Home*, l'avenir de cet espace d'intimité est questionné, par l'arrivée des objets connectés au sein du foyer.



REGARD SUR : LES FOYERS D'AUJOURD'HUI

La famille Brillaud vient de souscrire à l'offre datome.

Contre une rémunération mensuelle, la famille s'engage à utiliser exclusivement les services proposés par Netizon. Le géant du numérique s'assure ainsi l'exclusivité de la captation des données de ce foyer.

L'ouverture du pack de bienvenue réserve quelques surprises, avec de nouveaux objets connectés qui s'invitent chez les Brillaud.

Extrait d'un photo reportage sur les « Foyers d'aujourd'hui », la famille découvre le pack *datome*, après avoir signé un contrat d'exclusivité numérique avec *Netizon*.

Voir le tiré à part : https://linc.cnil.fr/vp2030

5 Philippe Ariès, *Histoire de la vie privée*, Seuil, 1985
6 Philippe Ariès, *Ibid.*
7 Stuart Shapiro, « Places and Spaces: The Historical Interaction of Technology, Home, and Privacy », *in Information Society*, vol. 14, no. 4, p. 275-284, 1998.
Traduit et cité par Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012
8 Entretien avec Antoine Prost, « Intime et public : de la construction à la confusion des frontières », *in Sciences Humaines*, 2003/7 (n°140)
9 Antoine Prost, « Frontières et espaces du privé », dans Philippe Ariès et Georges Duby (dir.), *Histoire de la vie privée*, Seuil, 1999

LA CONSTITUTION DE LA VIE PRIVÉE EN DROIT

Si elles tendent à se confondre depuis leur création, les notions de protection de la vie privée en France et de *privacy* aux États-Unis ont des origines et des approches différentes. L'antériorité de la reconnaissance de la protection de la vie privée reviendrait au droit français par rapport au droit américain[10]. Si elle est absente de la Déclaration des Droits de l'Homme et du Citoyen de 1789, il en est question dès 1791 lors de la révision de la Constitution et de l'insertion de garanties et limites à la liberté de la presse notamment pour ce qui relève des *« calomnies et injures contre quelques personnes que ce soit relatives aux actions de leur vie privée »*. La notion est reprise dans une loi sur la presse en 1819, puis dans la loi de 1881, pour ce qui relève de la diffamation. Aux États-Unis, la notion de *privacy* apparaît à la fin du XIX^{e} siècle avec une série de procès relatifs à l'usage publicitaire de noms de famille, ou de photographies sans l'autorisation des personnes concernées. James Whitman[11] différencie les visions européenne et étasunienne selon deux approches : dignité et liberté. La tradition européenne relèverait de la protection de la dignité, dans le prolongement de la notion d'honneur de l'ancien Régime, quand la tradition étasunienne serait centrée sur les libertés face à l'État – les faits démontrent que les deux approches coexistent des deux côtés de l'Atlantique.

Depuis l'Époque moderne, la montée en puissance de la protection de la vie privée comme un droit privé fondamental est indissociable de celle de l'individualisme dans nos sociétés. Elle est aussi liée à l'évolution des technologies qui en modifie les contours et empêche d'en fixer un contenu substantiel. L'imprimerie, la photographie, et le dévoilement d'informations privées qui en découle, va notamment conduire à la première formalisation du droit à la protection des données – *privacy* – par les juristes américains Warren et Brandeis en 1890. L'article publié par ces derniers constitue l'acte de naissance du droit à la vie privée dans sa conception anglo-saxonne et s'inscrit dans une conception libérale et bourgeoise de la société. Cette première dialectique entre droit et technologie illustre déjà l'impact de cette dernière sur la perception de la vie privée : en enregistrant, diffusant et conservant des informations ou des événements qui seraient uniquement restés dans la mémoire des participants, la technologie rend plus poreuse la frontière entre vie privée, confidentielle, et activités publiques, connues de tiers.

Warren et Brandeis formalisent ce nouveau droit, qu'ils définissent comme *« the right to be left alone »* (le droit d'être

Zoom sur…

Une typologie de la signification et des valeurs de la « privacy »

La « Stanford Encyclopedia of Philosophy Archive » propose une typologie des valeurs associées à la protection de la vie privée :

- **Contrôle des informations :** quand, comment et dans quelle mesure les informations nous concernant sont communiquées aux autres (Westin, 1967).
- **Dignité humaine :** ou inviolabilité de la personnalité humaine, définissant l'être humain (dignité, intégrité, autonomie, indépendance) (Bloustein, 1964).
- **Intimité :** contrôle des informations sur soi-même, permettant de maintenir divers degrés d'intimité dans les relations amoureuses, amicales et de confiance (Fried, 1970).
- **Relations sociales :** permet de développer des relations interpersonnelles diverses avec les autres, en protégeant ses biens et intérêts, ou se protéger de l'embarras, contre les conséquences délétères des fuites d'informations (Rachels, 1975).
- **Contrôle de l'accès à soi par d'autres :** accès physique, aux informations personnelles ou à l'attention, par l'anonymat notamment (Gavison, 1980), auxquels on peut ajouter l'accès au corps (Moore, 2003).

DeCew, Judith, «Privacy», *The Stanford Encyclopedia of Philosophy* (Spring 2018 Edition), Edward N. Zalta (ed.), https://plato.stanford.edu/archives/spr2018/entries/privacy/

10 Jean-Louis Halpérin, « Protection de la vie privée et privacy : deux traditions juridiques différentes ? », *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 48, no. 3, 2015, pp. 59-68.
11 James Whitman, « The Two Western Cultures of Privacy : Dignity v. Liberty », *The Yale Law Journal*, 2004, 113, p. 1151-1221.

laissé tranquille). Ce droit à la vie privée comme principe de non-intrusion est la base des législations de protection de la vie privée. Par exemple, la Déclaration universelle des droits de l'homme de 1948 indique dans son article 12 : *« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».*

> *« La vie privée correspond au contrôle sur les connaissances que les autres détiennent sur soi. »*
>
> *Charles Fried, Privacy, 1968*

L'arsenal juridique de protection de la vie privée définit cette dernière en opposition à la notion d'intrusion. Comme l'indique Bénédicte Rey, *« la vie privée est devenue une forteresse à défendre, au bénéfice d'un individu plongé dans des rapports de force déséquilibrés vis-à-vis des auteurs possibles d'intrusion »*[12]. La protection du domaine privé est construite contre les intrusions émanant alors essentiellement du gouvernement et des médias de masse.

Dans ce paradigme libéral, le droit à la vie privée est considéré comme un droit fondamental nécessaire à l'exercice des autres droits et libertés fondamentaux de nos régimes démocratiques : liberté d'opinion, liberté de circulation et de réunion, liberté syndicale, politique et de culte, le libre choix de ses mœurs et de ses relations sociales, etc. À l'échelle individuelle, la vie privée est indispensable à l'individu pour s'autodéterminer, se construire pleinement et cultiver son individualité[13].

Au cours du XXe siècle, cette conception libérale de la vie privée fondée sur la restriction de l'accès à la sphère privée va progressivement s'enrichir pour défendre le contrôle par l'individu des informations le concernant, comme en témoignent les définitions qu'en donnent les juristes américains Alan Westin, Charles Fried ou Arthur Miller dans les années1960.

Ainsi, l'individu doit être en mesure de contrôler les informations le concernant, de consentir ou de s'opposer à l'usage par autrui de ses informations personnelles. Ce droit à l'autodétermination informationnelle sera le socle des législations de protection des données personnelles élaborées à partir des années 1960 dans les pays occidentaux.

LA PROTECTION DES DONNÉES PERSONNELLES : UN DROIT À L'AUTO-DÉTERMINATION INFORMATIONNELLE

Ainsi, un droit de protection des données personnelles émerge dans les pays occidentaux. S'il s'inscrit dans la continuité du droit de protection de la vie privée, il l'élargit pour prendre en considération les relations entre l'informatique et la société. Plutôt que de se cantonner aux effets posés par l'informatique sur la vie privée, ce nouveau cadre législatif va interroger les libertés individuelles et collectives au regard du développement de cette technologie. Le droit à la protection des données personnelles répond aux inquiétudes liées au développement de l'informatique et des bases de données sur la liberté et l'autonomie des individus et doit permettre de rétablir la confiance – du citoyen et du consommateur – en l'informatique.

L'époque est alors aux imposants macroordinateurs (*mainframes*), produits des besoins du complexe militaro-industriel de la guerre froide et rapidement utilisés pour de multiples applications. Loin des utopies californiennes des années 1970 qui associent l'ordinateur à l'émancipation[14], l'informatique est perçue comme un danger et une menace pour les individus. Deux œuvres de science-fiction, très populaires à cette époque, illustrent cet imaginaire : *1984* de Georges Orwell (paru en 1949) et *2001, l'odyssée de l'espace* de Stanley Kubrick (1968). Elles contribuent à transformer l'image de l'ordinateur, qui n'est plus considéré uniquement comme un outil automatisant des tâches laborieuses de calculs mathématiques, mais qui devient une machine bureaucratique au service du contrôle rationalisé de la population – ou d'un équipage.

Dans les pays occidentaux, une coalition d'acteurs, essentiellement constituée de hauts fonctionnaires, va formaliser les principes – encore largement en vigueur – sur lesquels vont se fonder les droits nationaux de protection des données personnelles. Ce référentiel, que certains auteurs nomment le « paradigme de la vie privée[15] », s'inscrit dans la perspective libérale du droit à l'auto-détermination informationnelle (la libre disposition de ses données personnelles). Plutôt

12 Bénédicte Rey, « Vers un changement de perspective pour garantir le droit à la vie privée ? », *Les Cahiers du numérique* 2014/1 (Vol. 10), pages 9 à 18
13 Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, 1997
14 Fred Turner, *Aux sources de l'utopie numérique : De la contre-culture à la cyberculture, Stewart Brand, un homme d'influence*, C&F Editions, 2012
15 Colin J. Bennett and Charles Raab, *The Governance of Privacy. Policy Instruments in Global Perspective*, MIT Press, 2003

que de définir *a priori* ce qui relève de la sphère publique ou de la sphère privée, il suppose de laisser l'individu libre de décider de la circulation de ses données personnelles, en le dotant d'un ensemble de droits techniques[16]. Les données personnelles ne sont d'ailleurs pas uniquement les données relatives à l'intimité des individus, mais toute information qui puisse permettre d'identifier, directement ou indirectement, un individu. Ainsi, comme l'a rappelé la Cour de justice de l'Union européenne : « *les notions de données à caractère personnel […] et de données relatives à la vie privée ne se confondent pas* »[17]. Dès lors, si les sphères de protection des données personnelles et de la vie privée peuvent se recouper, elles présentent chacune des spécificités.

Zoom sur…

Protection de la vie privée ou protection des données ?

Souvent employée l'une pour l'autre, la protection des données personnelles et la protection de la vie privée relèvent de cadres juridiques distincts et leur périmètre diffère. Si, en France, la jurisprudence du Conseil constitutionnel n'a pas détaché la protection des données personnelles de celle de la vie privée, en Europe, la Charte des droits fondamentaux de l'Union européenne sépare les deux notions : l'article 7 consacre le respect de la vie privée, quand l'article 8 élève la protection des données personnelles comme droit fondamental.

La notion de vie privée est plutôt relative à l'intimité des personnes quand la protection des données est plus large, et intègre la vie privée. Il faut noter que la seule occurrence de l'expression « vie privée » dans le Règlement général à la protection des données (RGPD) figure dans le Considérant 4, qui lui-même renvoie vers la Charte des droits fondamentaux. Le terme *privacy* n'apparait pas dans la version anglaise, on retrouve uniquement celui de « *private and family life* ». On le retrouve par contre dans la directive e-Privacy, « vie privée et communications électroniques », relative au secret des communications, qui se recoupe avec le RGPD dans son application[18].

D'un point de vue pratique, le droit à la protection des données personnelles se traduit concrètement par un « ensemble de droits techniques » (information, accès, rectification, suppression, portabilité), quand le droit à la vie privée relève de l'identification de ce qui relève de la vie privée[19]. Si l'apparition puis le développement du numérique ont d'abord laissé penser que la protection des données personnelles devrait faire l'objet d'un droit autonome, la massification de données – dont la granularité est toujours plus fine – conduit certains auteurs comme Antoinette Rouvroy[20] à souhaiter un renforcement des liens entre données et vie privée. Dans les faits, l'application du RGPD et de la loi Informatique et Libertés le permet. La protection des données vient renforcer la protection du droit au respect de la vie privée pour en assurer l'effectivité.

Ainsi, des données qui ne relèvent pas directement de la sphère privée, voire des données publiques ou partagées publiquement par les individus, restent des données soumises à la protection des données. Elles demeurent protégées du fait de leur caractère personnel et leurs usages pourraient porter atteinte à l'identité humaine, aux droits de l'homme, à la vie privée, aux libertés individuelles ou publiques, selon les termes de l'article 1er de la Loi Informatique et Libertés.

Ainsi la protection des données a vocation à protéger la vie privée, mais parfois également la vie publique.

16 Tels que le droit à l'information, le droit d'accès, le droit de rectification, le droit d'opposition, le droit de ne pas faire l'objet d'une décision algorithmique, le droit au déréférencement et encore le droit à l'effacement.
17 CJUE, 16 juillet 2015, « ClienthEarth » Aff. C-615/13 P pt. 32, cité par Julien Rossi et Jean-Édouard Bigot. « Traces numériques et recherche scientifique au prisme du droit des données personnelles », *Les Enjeux de l'information et de la communication*, vol. 19/2, no. 2, 2018, pp. 161-177.
18 https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation
19 Audrey Bachert-Peretti, « La protection constitutionnelle des données personnelles : les limites de l'office du Conseil constitutionnel face à la révolution numérique », *Revue française de droit constitutionnel*, 2019/2 (N° 118), p. 261-284
20 Antoinette Rouvroy, « Homo juridicus est-il soluble dans les données ? », *Droit, normes et libertés dans le cybermonde*, Liber Amicorum Yves Poullet, Larcier 2016

Zoom sur…

Les critiques du paradigme libéral de la vie privée

Le paradigme libéral de la vie privée est aujourd'hui largement accepté, notamment par les industriels de l'économie numérique, qui négocient l'application de ses grands principes plutôt que de les remettre en cause. Il a pourtant fait l'objet de critiques d'inspirations diverses[21].

Les économistes de l'École de Chicago se sont opposés dès les années 1970 à toute forme de régulation des données personnelles. Ils perçoivent en effet dans le droit à la vie privée un obstacle au fonctionnement optimal des marchés, dans la mesure où celui-ci contraint la condition d'une transparence de l'information. Par ailleurs, la critique féministe dénonçait l'opposition binaire entre espace public et sphère privée, qui empêche de rendre public ce qui est considéré comme relevant du privé, comme par exemple, les violences domestiques, longtemps reléguées dans la sphère privée, limitant leur politisation.

Christian Fuchs critique également le « fétichisme » de la vie privée et l'aveuglement de la conception individualiste du paradigme libéral aux rapports de domination de classe et de genre. Selon lui, « *le capitalisme protège la vie privée des riches et des entreprises, mais légitime dans le même temps la violation de la vie privée des consommateurs et des citoyens* »[22].

Enfin, l'approche marxiste analyse la collecte des données personnelles en relation avec le développement du capitalisme informationnel. Dans cette optique, les individus sont pris dans un rapport d'exploitation au travers duquel ils subissent non seulement une intrusion dans leur sphère privée, mais en outre une aliénation à une forme de travail productif de données. Pour le contrer, il serait nécessaire selon eux de faire émerger un rapport de force collectif et d'envisager la protection des données personnelles au travers du régime des communs[23].

21 Julien Rossi, *Protection des données personnelles et droit à la vie privée : enquête sur la notion controversée de « donnée à caractère personnel »*, thèse de doctorat en sciences de l'information et de la communication, Université de Technologie de Compiègne, 2020
22 Christian Fuchs, « Towards an alternative concept of privacy », *Journal of Information, Communication and Ethics in Society*, vol. 9, n°4, p. 220-237
23 Laura Aufrère et Lionel Maurel, « Pour une protection sociale des données personnelles », 2018 https://scinfolex.com/2018/02/05/pour-une-protection-sociale-des-donnees-personnelles
24 http://www.le-tigre.net/marc-l.html

Diversité des pratiques et des comportements en matière de protection des données

« Bon anniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc ? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du Tigre. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet. (…) Je préfère te prévenir : ce sera violemment impudique, à l'opposé de tout ce qu'on défend dans Le Tigre. »

En 2008, le journal Le Tigre[24] dressait le portrait d'un inconnu à partir des traces librement accessibles sur Internet afin d'alerter sur le fait qu'une fois rassemblées, des informations éparses et *a priori* insignifiantes, offraient une description fine de la vie d'un individu.

Diversité des pratiques et des comportements en matière de protection des données

Nos pratiques numériques sont profondément sociales.
Elles sont inscrites dans des rapports de domination et insérées
dans des structures socio-économiques, qui entravent les capacités effectives
des individus à maîtriser les flux des informations les concernant.

DE L'INTRUSION À L'EXPOSITION DE SOI : LA DIVERSITÉ DES PRATIQUES NUMÉRIQUES ET DE PROTECTION DES DONNÉES PERSONNELLES

Pexels cc-by Aleksandar Pasaric

La fin de la vie privée ?

Face à l'essor de la collecte des traces relatives aux faits, gestes et préférences des individus par les firmes commerciales et à leur exposition sur les réseaux sociaux, plusieurs auteurs ont conclu à la « fin de la vie privée ». Mark Zuckerberg ou Eric Schmidt ont défendu au début des années 2010 que la vie privée était une notion obsolète. Ces discours, qui justifient leurs propres choix commerciaux de valorisation des traces de leurs utilisateurs, s'opposent pourtant aux pratiques des individus. S'exprimer sur un espace public en ligne ou tout acte d'exposition de soi n'est pas incompatible avec le souhait et le fait d'avoir une vie privée.

Les enquêtes empiriques sur les pratiques numériques contredisent ces affirmations comme le défendent les sociologues Alice Marwick et danah boyd : « *Les gens se soucient profondément du respect de la vie privée et développent des stratégies innovantes pour y parvenir tout en participant aux systèmes qui leur permettent d'accéder aux informations, de socialiser avec leurs amis et d'interagir avec les plateformes de divertissement contemporaines* »[25]. Les individus développent des stratégies pour contrôler les informations qu'ils souhaitent diffuser et à qui, en veillant à la façon dont elles seront reçues et interprétées. Toutefois, ils n'ont pas toutes les cartes en main pour maîtriser ces flux informationnels, largement inscrits dans des structures socio-économiques sur lesquelles ils n'ont que peu de prises. Comme l'analyse le sociologue Antonio Casilli, la vie privée est négociée, au cas par cas, selon les situations[26].

25 Alice E. Marwick, danah boyd, « Understanding Privacy at the Margins », *International Journal of Communication*, 12(2018), 1157–1165
26 Antonio A. Casilli, « Contre l'hypothèse de la « fin de la vie privée » », *Revue française des sciences de l'information et de la communication*, 3, 2013

FUTUR SPÉCULATIF

Home Sour Home

Dans ce scénario, sont explorées les nouvelles pratiques de dévoilement et de maîtrise de ses données en 2032.

REGARD SUR : LES FOYERS D'AUJOURD'HUI

Marion et Théo sont adeptes du Grand Oubli. Tous les jours, à 22h, ils se connectent à leurs gestionnaires de données respectifs.

Le rituel est immuable, chacun est installé dans son coin et passe en revue les données produites au cours de la journée.

Sans concertation et dans un silence total, Marion et Théo décident lesquelles de leurs données personnelles sont effacées ou conservées.

Extrait d'un photoreportage sur les « Foyers d'aujourd'hui », avec un couple adepte de la pratique du « Grand Oubli ».

https://linc.cnil.fr/vp2030

De nombreux travaux universitaires traitent des pratiques d'exposition de soi sur les réseaux sociaux[27]. Ils mettent en évidence le fait que les individus font un usage stratégique du dévoilement d'informations personnelles pour se construire une identité (en ligne ou hors ligne) et un capital social. Toutefois, la visibilité des individus dépend de leur savoir-faire, de leur maîtrise de l'outil et de la compréhension de ses normes. Il existe ainsi une inégalité qui sépare le profane de l'initié. La volonté de contrôle de son image varie également selon les caractéristiques sociales des individus. Par exemple, plusieurs travaux sur les usages numériques des adolescents ont montré qu'elle était plus importante chez les jeunes filles que chez les garçons[28], et surtout qu'il est plus complexe et plus ardu pour une femme de contrôler sa visibilité en ligne[29]. Ces études pointent également que la réflexivité sur leurs pratiques numériques croît avec l'âge. Dominique Pasquier constate que la recherche de la notoriété en ligne n'est pas au cœur des pratiques numériques des classes populaires, dont la « pudeur participative » les conduit à privilégier les échanges avec leurs proches[30].

Enfin, les capacités à mettre en œuvre ces stratégies de négociation de sa vie privée sont inégales selon les individus. Cela nécessite d'une part des compétences techniques quant aux principes de fonctionnement des systèmes utilisés quotidiennement ; d'autre part, cela requiert de maîtriser les codes de différents milieux sociaux. Il est souvent difficile de comprendre quelle peut être la norme dans une situation donnée. Benjamin Bitane, responsable des formations chez Emmaüs Connect, remarque cette problématique chez certaines populations jeunes qui ont un usage récréatif du numérique, mais un rapport difficile sur d'autres sujets. *« Ils maîtrisent aujourd'hui leur image sur les réseaux sociaux par rapport à leur vie quotidienne et leur groupe de pairs. Mais ce qu'ils ne maîtrisent pas du tout est le caractère poreux de leur image, quand ça change de monde social. On a du mal à leur faire comprendre que la boîte mail bg75@coucou.fr ne convient pas, ou que la vidéo sur Youtube où ils sont bourrés avec des potes, leur futur employeur peut tomber dessus. Donc, s'ils sont très à l'aise sur les réseaux sociaux, ils n'ont pas du tout les us et coutumes du numérique "sérieux", les codes traditionnels »*[31]. Ces situations « d'effondrement de contexte[32] », où nos sphères sociales entrent en collision, ne sont pas propres au numérique, mais elles se sont accentuées avec les réseaux sociaux. Or, l'habileté à gérer une représentation de soi multiple et à naviguer entre les mondes sociaux est inégalement développée parmi les individus. Jongler entre différents environnements et identités requiert une prise de recul et des compétences spécifiques, une compréhension des normes et des pratiques des communautés et une habileté pour se présenter de manière cohérente dans les différents environnements dans lesquels nous interagissons. Cette difficulté est en outre renforcée par le caractère en réseau de l'environnement numérique : *« Les contextes ne s'effondrent pas par hasard ; ils se dissolvent parce que les individus ont des conceptions différentes de l'existence des frontières et de la façon dont leurs décisions affectent les autres*[33] ». Chaque personne peut

27 Voir notamment, Dominique Cardon, « Le design de la visibilité. Un essai de cartographie du web 2.0 », *Réseaux*, 2008/6 (n° 152), p. 93-137.

28 Voir notamment : Metton-Gayon Céline. Les adolescents, leur téléphone et Internet. « Tu viens sur MSN ? » Paris : L'Harmattan, 2009, 202 p & Bruna, Yann. « Snapchat à l'adolescence. Entre adhésion et résistances », *Réseaux*, vol. 222, no. 4, 2020, pp. 139-164.

29 Alice Marwick, (2013) "Gender, Sexuality and Social Media." In Senft, T. & Hunsinger, J. (eds), *The Social Media Handbook*. Routledge, 2013, pp. 59-75.

30 Dominique Pasquier, *L'Internet des familles modestes. Enquête dans la France rurale*, Presses des Mines, 2018, 222 p

31 Lors d'un entretien avec le LINC, 12 mars 2020

32 danah Boyd, *C'est compliqué : les vies numériques des adolescents*, C & F éditions, 2016

33 danah Boyd, *Ibid.*, p. 118

avoir une vision claire de ce qui est approprié dans une situation particulière, mais ses amis ne partagent pas forcément sa conception de ces normes sociales.

Des pratiques profanes de protection de ses données

Au-delà des dynamiques d'expression sur les réseaux sociaux, les personnes exploitent les interstices et les angles morts des infrastructures et des pratiques de surveillance pour se forger des espaces à soi, préserver leur intimité, s'accorder des moments de répit, jouer avec ce qu'ils souhaitent cacher ou dévoiler. Sans être des experts techniques, ils font preuve de créativité face aux dispositifs sociotechniques pour protéger leur intimité. Dans l'ombre des savoirs légitimes, ils mettent en œuvre des tactiques et développent des compétences profanes en matière de protection de leurs données personnelles, plus ou moins proches des normes recommandées, et, s'appuyant sur un savoir pratique davantage que sur des connaissances techniques ou juridiques. À ce titre, la créativité des individus pour protéger leur vie privée et leurs données est grande : morceau de scotch sur la webcam, étuis bricolés pour éviter les fraudes au paiement sans contact, installation d'un bloqueur de publicité, fourniture de fausses informations dans les formulaires en ligne, comptes multiples ou partagés, recours aux pseudos, utilisation de plusieurs adresses email selon les usages, inscription sur liste rouge, suppression régulière des cookies, etc. Si l'efficacité de ces dispositifs est variable, ils témoignent d'un malaise et d'une crainte vis-à-vis de la collecte non autorisée de données. Ce foisonnement de stratégies d'autoprotection est, de plus, rendu particulièrement nécessaire par la très grande uniformité des offres de services numériques : du fait du caractère global des entreprises qui les proposent et des économies d'échelle qu'elles procurent, celles-ci sont pensées sur un modèle unique pour le monde entier, généralement issu des besoins et des attentes du marché étatsunien. L'absence de spécificités régionales ou nationales et l'impossibilité de personnaliser les traitements et les services ou d'avoir accès à une alternative pousse les individus à contourner ou détourner ce qui est à leur main (le matériel, les champs d'un formulaire, etc.).

> *« Quand tu demandes à un ado : « est ce que je peux voir ton compte ? », il te demande « lequel tu veux ? ». En général, il en a deux ou trois, il y a celui pour les parents, celui pour l'école et celui pour les copains. Avec des identités bien différentes. Ça témoigne non seulement d'une conscience de la conséquence de son image en ligne, ça témoigne d'une réflexivité et ça témoigne d'une capacité à agir. »*
>
> *Anne Cordier*[34]

Des post-it aux caches webcam devenus des objets promotionnels : des pratiques quotidiennes de protection de sa vie privée.

34 Xavier de la Porte, interview d'Anne Cordier, Sommes-nous en train de fabriquer des « crétins digitaux » ?, *Podcast : Le code a changé*, France Inter, https://www.franceinter.fr/emissions/le-code-a-change/sommes-nous-vraiment-en-train-de-fabriquer-des-cretins-digitaux

Des pratiques numériques ancrées dans des relations sociales

Alors qu'ils sont souvent accusés de se dévoiler en méconnaissance de cause, les travaux sur les pratiques numériques de la population adolescente témoignent d'une réflexivité et d'une compréhension du modèle économique des services qu'ils utilisent. Il faut se défaire des idées reçues selon lesquelles les jeunes, les moins éduqués ou les plus précaires seraient moins vigilants quant à la vie privée et auraient des comportements laxistes ou négligents en matière de protection de leurs informations personnelles. Ces discours moralisateurs opèrent une réduction du problème à une dimension individuelle et tendent à occulter les conditions qui favorisent la diffusion d'informations personnelles dans les pratiques quotidiennes des individus. Cette orientation morale, voire paternaliste, centrée sur le comportement individuel omet le fait que protéger sa vie privée et ses données personnelles ne relève pas toujours, voire même rarement, d'une simple décision individuelle, mais d'arbitrages complexes dans des conditions sociales pouvant être difficiles.

> *« Si on veut échapper à la collecte de nos données, on est marginalisé. »*
>
> *Cristina Machado* [35]

Les individus sont en effet insérés dans des relations sociales qui déterminent leurs usages du numérique. Par exemple, recourir à ses droits sociaux requiert d'avoir une adresse email et de dévoiler des informations. Stéphane Koukoui, médiateur numérique à Rennes, témoigne : *« Il est difficile de se soustraire à la pression des GAFAM. Tu vas dans un centre social, tu dis que tu n'as pas de boîte email et que tu en voudrais une pour te créer ton compte sur Pôle emploi, ils vont t'ouvrir une boîte sur gmail*[36] *»*. Autre exemple, comme le pointe l'anthropologue Pascal Plantard, s'intégrer au sein d'un groupe social peut nécessiter d'utiliser des réseaux sociaux : *« les socialisations adolescentes ne font plus la différence entre les normes sociales ordinaires et les normes sociales numériques. Les réseaux sociaux sont devenus des espaces où on parle à ses amis, comme à l'école ou sur un terrain de foot. Les ados en ont besoin pour ne pas se sentir exclus du groupe et pour discuter entre eux, loin du regard des parents*[37] ».

Travailler pour une entreprise ou une organisation peut également conduire à se voir imposer des outils dont on ne partage pas les principes, même lorsque l'on a pour habitude d'être très vigilant, à l'image de Antonio Casilli : *« [avec le confinement] Il s'est joué à mon sens ce qui se joue depuis 15 ans. On ne lâche rien au niveau de notre vie privée, mais on choisit les batailles que l'on peut gagner. Par contre, dans certains cas, on est obligé à des retraites stratégiques. Je pense à l'usage de certains outils comme Zoom. […] Personnellement, c'est mon employeur qui me l'a proposé. C'est ça ou il n'y a pas de communication. On peut composer, mettre en place des stratégies pour limiter les dégâts, par exemple choisir l'équipement qui se connecte ou choisir l'endroit d'où on se connecte et ainsi de suite. Mais il y a des moments où l'on peut difficilement faire autrement*[38] ».

Nos pratiques numériques sont ainsi ancrées dans des relations sociales et des structures socio-économiques. Il est difficile pour un individu d'avoir des pratiques économes en données quand toute l'économie semble rechercher la captation d'un maximum de données sur l'individu. Les incitations à se dévoiler sont permanentes et les effets de réseau, qui renforcent la concentration des activités sur quelques outils, rendent particulièrement difficile de s'abstraire des dynamiques collectives. Surtout, les technologies numériques ayant pénétré l'ensemble de nos environnements, on habite le numérique même lorsque nos pratiques ne le sont pas : se promener dans la rue signifie aujourd'hui inévitablement laisser un certain nombre de traces. Ne pas être sur un réseau social ne signifie pas que nous n'ayons pas d'existence numérique.

En 2019, la journaliste Kashmir Hill a tenté l'expérience de se passer des GAFAM pendant plusieurs semaines[39]. Cela s'est avéré particulièrement ardu tant ces entreprises constituent des infrastructures sur lesquelles reposent une large part des services numériques. Par exemple, se couper d'Amazon signifie perdre accès à tous les sites hébergés par Amazon Web Services, le premier fournisseur de cloud. Refuser Google, c'est s'interdire l'accès à tous les sites et applications qui utilisent les services de l'entreprise pour afficher de la publicité, publier une carte Google Maps, suivre leurs utilisateurs ou encore déterminer si les visiteurs sont des humains ou des robots. Elle conclut : *« Une fois l'expérience terminée, j'ai recommencé à utiliser les services de ces entreprises car, comme je l'ai démontré, je n'avais pas vraiment d'autre choix*[40] ». Dès lors, plutôt qu'un *« privacy paradox*[41] » qui suppose une liberté de choix, les individus se résignent en l'absence de prises concrètes leur permettant d'exercer une action sur la circulation de leurs données[42].

35 Lors d'un entretien avec le LINC, 13 octobre 2020
36 Cité par https://labs.letemps.ch/interactive/2020/longread-donnees-personnelles/
37 https://www.liberation.fr/debats/2020/09/10/pour-les-collegiens-etre-populaire-peut-etre-lie-a-avoir-des-flammes-sur-snapchat_1799108
38 Xavier de la Porte, interview de Antonio Casilli, COVID, confinement et grande conversion numérique, avec Antonio Casilli, *Podcast : Le code a changé*, France Inter https://www.franceinter.fr/emissions/le-code-a-change/covid-confinement-et-grande-conversion-numerique-avec-antonio-casilli
39 Kashmir Hill, « I Cut the 'Big Five' Tech Giants From My Life. It Was Hell », *Gizmodo*, juillet 2019, https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194
40 Kashmir Hill, « I Tried to Live Without the Tech Giants. It Was Impossible. », *New-York Times*, juillet 2020 https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html
41 Le « *privacy paradox* » correspond à la contradiction entre l'inquiétude déclarée des individus pour la collecte de leurs données personnelles et leurs pratiques courantes de partage d'informations.
42 Draper, N. A. and Turow, J. (2019) « The corporate cultivation of digital resignation », *New Media & Society*, 21(8), pp. 1824–1839

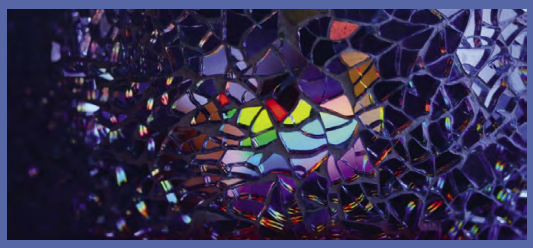
Moins dotés, mais plus collectés

Les sociologues danah boyd et Alice Marwick soulignent à quel point la protection de la vie privée est une lutte quotidienne, dont certaines populations, inscrites dans des rapports de pouvoir défavorables, sortent rarement victorieuses[43]. Avec la numérisation toujours croissante de nos sociétés, la possibilité « d'*opt out* » des systèmes automatisés devient de plus en plus un privilège. Si pour certains la collecte des données est consentie, pour d'autres elle est subie. Parce qu'ils ont moins de pouvoir pour y résister, certains groupes sociaux sont davantage ciblés par des programmes intrusifs.

L'exemple du recours aux droits sociaux témoigne des contraintes qui pèsent sur la maîtrise de leurs informations par les individus. Les bénéficiaires n'ont en effet pas d'autre choix que d'entrer dans un régime de transparence vis-à-vis de leurs pratiques pour recourir à leurs droits sociaux. Comme l'explique Héléna Revil, politiste au sein de l'Observatoire des non-recours aux droits et services (ODENORE) : « *Recourir aux droits, c'est d'une certaine manière se donner à voir, c'est se rendre visible. Pour accéder à certaines prestations, aides, services, ciblés sur différents critères, on doit donner des pièces justificatives, en nombre parfois important. Les personnes peuvent se sentir mises à nu. Quand on n'est pas dans une situation de vulnérabilité, on ne se rend pas compte de cette nécessité de s'exposer*[44] ». Dans la lutte contre la fraude aux prestations sociales, cette intrusion dans la sphère privée des individus est croissante, sans que les usagers n'aient toujours conscience du transfert de leurs données à d'autres administrations, comme le déplore le Défenseur des Droits. « *Force est de constater que les modalités d'utilisation de la coopération inter-organismes et du droit de communication mentionnées dans les formulaires de demande de prestation des CAF ou des caisses MSA n'apparaissent qu'en bas de page, dans une police réduite, bien que ces modalités de contrôle soient le pendant du versement de la prestation*[45] ». Outre les données administratives qui sont progressivement partagées entre les organismes sociaux, cet impératif de transparence tend à s'étendre à toujours plus d'aspects de la vie quotidienne. L'instauration d'un « droit de communication » offre aux agents chargés du contrôle dans les organismes – étendus aux agents de Pôle Emploi avec le projet de loi de Finances 2021[46] – le pouvoir de solliciter diverses pièces auprès des établissements bancaires, des opérateurs téléphoniques ou des fournisseurs d'énergie. Certaines administrations vont même au-delà de leurs habilitations comme le dénonce le Défenseur des Droits. « *Certains conseils départementaux ont également exigé la production des attestations d'assurance auto, moto et habitation des bénéficiaires. Ces pièces n'ont aucune utilité pour le contrôle des conditions d'ouverture ou le calcul du montant du RSA, elles permettent cependant d'apprécier le train de vie de l'allocataire*[47] ».

Pour la juriste américaine Michele E. Gilman, les populations les plus précaires sont tenues d'échanger leur vie privée contre l'accès aux droits sociaux. Elle en conclut que les Américains pauvres vivent la vie privée différemment des personnes disposant de ressources économiques plus importantes. En matière de droit à la vie privée, il existe des différences de classe sociale[48].

FRAGMENT D'IMAGINAIRES



« Rendant compte de deux expériences successives pendant lesquelles l'artiste Mark Farid a, d'abord, pratiquement disparu du monde numérique, puis ensuite, réapparu en rendant publique la totalité de ses traces numériques, y compris bien sûr celles qui concernaient ses interactions avec des tiers. Sa conclusion : il est beaucoup plus pénible d'être invisible que d'être surexposé, y compris d'un point de vue psychologique. Mais il relie cela à la manière dont le numérique s'organise et organise le monde : beaucoup de fonctions de la vie ne sont plus accessibles en dehors du numérique, et l'exposition publique oriente nos pratiques dans des directions que nous savons socialement valorisantes, créant une forme de satisfaction dépourvue de tout réflexivité. Pour Farid, certes, on ne peut pas « vivre » aujourd'hui sans abandonner ses données au profit des plateformes numériques, mais cela rend des choix politiques d'autant plus nécessaires : l'échelle individuelle n'est pas la bonne pour reconstituer des marges de manœuvre. »

Voir le tiré à part : https://linc.cnil.fr/vp2030

43 Alice E. Marwick, danah boyd, « Understanding Privacy at the Margins », *International Journal of Communication* 12(2018), 1157–1165

44 Lors d'un entretien avec LINC (24 novembre 2020)

45 Rapport *Lutte contre la fraude aux prestations sociales : à quel prix pour les droits des usagers ?*, Défenseur des droits, 2017, p. 20

46 Bertrand Bissuel, « Pôle emploi obtient de nouveaux pouvoirs pour combattre la fraude », *Le Monde*, décembre 2020, https://www.lemonde.fr/politique/article/2020/12/19/pole-emploi-obtientde-nouveaux-pouvoirs-pour-combattre-la-fraude_6063941_823448.html

47 Rapport *Lutte contre la fraude aux prestations sociales : à quel prix pour les droits des usagers ?*, Défenseur des droits, 2017, p. 24

48 Michele E. Gilman, « The Class Differential in Privacy Law ». Brooklyn *Law Review*, Vol. 77, No. 4, Summer 2012, Available at SSRN: https://ssrn.com/abstract=2182773

TIRÉ À PART

Du fragment d'imaginaire à l'artefact spéculatif, des fictions pour explorer les futurs

En parallèle de ce cahier Innovation et prospective, nous publions en ligne un tiré à part visant à retracer les différents futurs de la privée à l'horizon 2030. Une exploration prospective et spéculative réalisée à l'initiative du LINC, accompagné par les studios Casus Ludi / Design Friction, Chronos et Daniel Kaplan, ainsi que des experts de tous horizons.

Cette exploration vise à proposer de nouveaux récits et imaginaires qui permettent d'interroger la protection des données personnelles à l'horizon 2030 et d'apporter une réflexivité sur les pratiques de régulation.

Tout au long de la démarche, nous avons cherché à mettre en évidence les frictions qui pourraient être déclenchées par les usages des technologies dans différents groupes sociaux et moments de la vie numérique, ainsi que les risques qui en découleraient pour les libertés individuelles et collectives.

Trois approches complémentaires sont mobilisées – les imaginaires, la fiction spéculative et le design fiction – pour l'exploration de quatre axes complémentaires et qui se croisent : la vie quotidienne, les pratiques numériques ordinaires, les inégalités et les différenciations sociales, la relation à la vie privée.

Ce document de 80 pages retranscrit ces explorations avec notamment une « analyse de fragments fictionnels et artistiques » collectés à la suite d'un appel lancé en août 2020 auprès des internautes, puis « trois futurs spéculatifs pour la vie privée en 2030 » : Réputé ou répudié, L'ingérence face aux ingérables, Home Sour Home.

Vous pourrez en retrouver des extraits dans ce cahier, sous forme d'encadré, et parcourir cette exploration en ligne.

Télécharger le tiré à part : https://linc.cnil.fr/vp2030

POURQUOI AVONS-NOUS DES COMPORTEMENTS DIFFÉRENTS EN MATIÈRE DE PROTECTION DE NOS DONNÉES ?

La protection des données personnelles, et notamment le RGPD, vise à faire respecter les droits fondamentaux de chacun des individus. Pour cela, elle attribue des droits aux individus et des obligations aux responsables de traitement et aux sous-traitants, que sont les entreprises et toutes les organisations amenées à collecter et à traiter des données. Les personnes ont ainsi des droits, y compris celui d'utiliser des services basés sur la collecte de leurs données, et surtout celui de pouvoir changer d'avis. Charge aux entreprises de le leur permettre. La responsabilité *in fine* reste toujours celle du « responsable de traitement ». Cependant, les torts causés aux personnes par des erreurs de gestion de leurs données, et de leur image, peut avoir des conséquences négatives, qui bien souvent ne relèvent juridiquement pas de la protection des données, notamment pour ce qui a trait à l'intimité, et aux réseaux sociaux par exemple. Pour ces raisons, la protection des données s'accompagne d'une politique de prévention des personnes afin de limiter le risque de devenir victime.

Cette politique de prévention à l'égard de la protection des données repose notamment sur la capacité à mettre en œuvre les mesures appropriées pour se prémunir d'usages malveillants. Pour cela, un ensemble de prescriptions vise à rendre les individus plus prévoyants et à adopter une « culture du risque » vis-à-vis de leurs données personnelles, c'est-à-dire à anticiper les conséquences futures de leurs pratiques individuelles. Pour certains, cela peut prendre la forme d'injonctions à la prévoyance, parfois par la condamnation morale de comportements jugés insouciants, par exemple avec la stigmatisation des pratiques des adolescents sur les réseaux sociaux (page 18). Mais cela peut correspondre à des formes plus positives et fécondes de valorisation de « bonnes pratiques » en matière de protection de la vie privée et des données personnelles. Si les individus développent des compétences profanes de protection des données, les dispositifs de formation au numérique[49] – des enfants scolarisés aux populations éloignées du numérique – visent à faire intérioriser à ces individus de nouvelles pratiques numériques permettant d'éviter quelques écueils : créer un mot de passe sécurisé, paramétrer son navigateur et les comptes de ses services numériques, gérer finement les consentements, maîtriser son identité en ligne, utiliser un pseudonyme, etc.

Si beaucoup de personnes appliquent ces normes de prévention, leur mise en œuvre reste délicate. Il ne suffit pas de passer le message pour que les individus adoptent facilement les « bonnes » pratiques et les « bons » comportements. Tous les individus ne sont pas exposés au message de prévention de la même manière, les conditions de réception de celui-ci diffèrent, et, enfin, tous ne sont pas égaux pour l'appliquer. Les travaux menés dans les champs de la santé, de l'environnement, de l'alimentation ou de la sécurité routière mettent en évidence le fait que les messages sont diversement reçus selon les contextes sociaux, les styles de vie et les ressources matérielles et symboliques des individus[50]. Si le principe de prévoyance se présente comme universel, être prévoyant relève de dispositions inégalement distribuées[51]. On peut faire l'hypothèse que ces résultats s'appliquent dans le cas de la protection des données personnelles, et qu'il conviendrait de les prendre en compte pour l'accompagnement des personnes.

Politiques de prévention et tensions normatives

Les politiques de prévention, d'autant plus si elles reposent sur une forme de stigmatisation, comportent une part de violence symbolique lorsqu'elles incitent les individus à changer leurs pratiques sans prendre en considération les normes et les valeurs sur lesquelles reposent ces pratiques. La mise en œuvre des bonnes manières de protéger ses données personnelles met en jeu des valeurs et des intérêts contradictoires qui ne sont souvent ni clairement exposés ni débattus. En situation, la protection des données peut rarement être isolée d'autres considérations. Les individus sont confrontés à de multiples microdécisions qu'ils ont à prendre sans que le risque pour leur vie privée soit toujours priorisé par rapport aux différentes normes sociales qui pèsent sur eux. En effet, cet objectif peut entrer en tension avec d'autres impératifs et intérêts en jeu dans les différentes sphères de leur existence (la vie professionnelle, amicale, familiale ou publique). Par exemple, des tensions normatives entre le souci de protéger la vie privée et le risque de provoquer un conflit avec son employeur ou de mettre en cause l'harmonie familiale

49 Voir par exemple, les recommandations disponibles sur le site de la CNIL (https://www.cnil.fr/fr/maitriser-mes-donnees) ou les fiches à destination des formateurs conçues par Les Bons Clics (https://www.lesbonsclics.fr)

50 Benoît Bastard, « Quel sens donner aux comportements à risque face au Covid-19 ? », *AOC*, 5 juin 2020, https://aoc.media/analyse/2020/06/04/quel-sens-donner-aux-comportements-a-risque-face-au-covid-19/

51 Jean-Baptiste Comby, Matthieu Grossetête, « « Se montrer prévoyant » : une norme sociale diversement appropriée », *Sociologie*, 2012/3 (Vol. 3), p. 251-266. https://www.cairn.info/revue-sociologie-2012-3-page-251.htm

vont conduire le plus souvent à privilégier les seconds au détriment de la première. Comme le synthétise le sociologue Amitai Etzioni, *« La privacy doit trouver sa place parmi tout un ensemble de valeurs qui nous sont chères et qui ne sont pas toujours entièrement compatibles. C'est pourquoi nous devrions toujours peser l'importance que nous sommes prêts à accorder à la privacy, et l'importance que nous sommes prêts à accorder à d'autres valeurs, et en particulier à la protection de nos familles, de nos communautés et de notre patrie*[52] *».*

Comme l'indique la sociologue Dominique Pasquier, ces dissonances normatives sont particulièrement visibles au sein des classes populaires qu'elle a étudiées. *« Il y a une tension entre le familialisme des classes populaires et le caractère individuel des outils (le téléphone, l'adresse email, le mot de passe, etc.) qui mettent à l'épreuve les valeurs des classes populaires. Dans mon enquête, le collectif familial l'emporte sur la vie individuelle, il y a des tentatives de désindividualiser les outils. On s'échange les téléphones, on partage une même adresse email entre conjoints voire même pour toute la famille, et on est systématiquement « amis » sur Facebook. Partager les mots de passe est un principe de vie collective. Ne pas donner le mot de passe de son compte ou de son téléphone va être perçu comme un signe de tromperie ou de dissimulation. Ce n'est pas correct*[54] *».* Si elle invite à approfondir les enquêtes sur les spécificités du rapport aux informations personnelles selon les milieux sociaux, cette observation illustre que la question de la protection des données ne peut être envisagée seulement dans une perspective individuelle. Les individus sont insérés dans un cadre familial ou amical dont les valeurs et les attendus peuvent les conduire à partager un mot de passe ou laisser accès à leur compte Facebook ou SnapChat pour prouver sa loyauté et sa confiance[55]. Face à d'autres valeurs et impératifs, les frontières du privé peuvent ainsi être restreintes.

En outre, les solutions proposées peuvent être jugées contraignantes et difficiles à appliquer. Les « bonnes » pratiques peuvent bouleverser des usages routinisés du numérique. Cela peut conduire dès lors à une distanciation vis-à-vis de ces normes de protection de la vie privée : discours critique, rejet de certains services jugés trop contraignants, maintien de pratiques alternatives, jeu avec les recommandations pour les adapter à leur univers de contraintes professionnelles ou familiales, arrangements avec la norme, etc. Dès lors, le lien causal entre la connaissance des principes de protection des données et la mise en œuvre de pratiques conformes à ceux-ci est à modérer. On sait qu'en l'absence de mots de passe sécurisés, on s'expose à un risque de piratage de ses comptes numériques. Pourtant, il est difficile pour une large part d'entre nous de mettre en œuvre cette recommandation. Par exemple, les difficultés de mémorisation de mots de passe complexes et multiples nous conduisent à privilégier la simplicité de mots de passe semblables plus aisément mémorisables ou à les consigner dans un « carnet à mots de passe » qui, perdu ou révélé à un tiers, peut être dommageable. Ces comportements ne sont pas irrationnels. Au contraire, nous avons tous de bonnes raisons pour ne pas adopter les normes en matière de protection de nos données. Pour que les messages de prévention soient les plus pertinents possibles, il est nécessaire de comprendre ces raisons et le sens que nous accordons à ces pratiques.

> *« C'est très dur [de mettre en œuvre des pratiques de protection de nos données] car nos pratiques numériques sont très ancrées dans nos habitudes. Pour certains, le simple changement d'icône de leur webmail est très compliqué. C'est une vraie violence de changer nos habitudes »*[53]
>
> *Pierre-André Souville, Médiateur numérique, Rennes*

Les instances de socialisation à la protection des données

Les groupes sociaux dans lesquels nous sommes insérés jouent un rôle central dans la socialisation individuelle à la protection de nos données personnelles. D'une part, nos valeurs sont fortement nourries par la socialisation familiale antérieure (cf. supra). D'autre part, l'insertion dans des réseaux familiaux, professionnels, politiques ou amicaux donne accès à des ressources, à un « capital informatique[56] » et fait sensiblement évoluer les pratiques en matière de protection des données. Le travail longitudinal réalisé par la sociologue Anne Cordier, qui suit des jeunes sur plusieurs années, témoigne que l'évolution de leurs stratégies et pratiques en matière de protection des données personnelles est étroitement liée à leur insertion dans différents cercles de sociabilité[57]. Par exemple, une jeune femme militante dans un mouvement antifasciste a transformé radicalement ses pratiques en matière de protection de ses données.

52 Amitai Etzioni, *The limits of privacy*, Basic Books, 1999, p. 260
53 Lors d'un échange avec le LINC, 1er octobre 2020
54 LINC.cnil.fr, entretien avec Dominique Pasquier, « *Dans les classes populaires, la vie privée relève moins de l'individu que du groupe familial* », mars 2020 https://linc.cnil.fr/fr/dominique-pasquier-dans-les-classes-populaires-la-vie-privee-releve-moins-de-lindividu-que-du-groupe
55 Margot Déage, « S'exposer sur un réseau fantôme. Snapchat et la réputation des collégiens en milieu populaire », *Réseaux*, 2018/2-3 (n° 208-209), p. 147-172.
56 Cédric Fluckiger, « Les collégiens et la transmission familiale d'un capital informatique », *Agora débats/jeunesses*, 2007/4 (N° 46), p. 32-42
57 Anne Cordier, « Du design de la transparence à l'agir informationnel : Les apports d'une approche sociale de l'information », 2017

Les individus s'adaptent ainsi aux normes sociales attendues par un milieu social. De même, les pratiques imposées dans le cadre professionnel peuvent mener à des transferts de compétences dans les pratiques personnelles.

FRAGMENT D'IMAGINAIRES

« Le scénario Uninvited Guest, du studio Superflux, montre une personne âgée obligée de bricoler des stratagèmes pour vivre la vie qu'elle a choisie malgré les injonctions des multiples objets connectés que sa famille (aimante) l'a contraint d'utiliser. »

Voir le tiré à part : https://linc.cnil.fr/vp2030

Les proches jouent ainsi un rôle crucial dans l'apprentissage de pratiques de protection des données par l'entraide et le partage de bonnes pratiques. Irène Bastard constate que les aînés des fratries encadrent les premiers pas sur Facebook des adolescents et leur transmettent les codes et pratiques générationnelles[58]. Pierre-André Souville, médiateur numérique à Rennes confirme : *« l'apprentissage se fait beaucoup par les pairs. Le discours est plus efficace quand ça vient de notre entourage. Les enfants, les amis, les voisins ou les collègues sont les premières personnes vers qui les gens se tournent quand ils ont un problème avec le numérique[59] »*. L'enquête Capacity a également mis en évidence que le facteur clé d'exclusion numérique n'est pas la catégorie sociale mais l'isolement comme nous l'indique le coordinateur de ce projet de recherche, Jacques-François Marchandise : *« Les personnes socialisées s'en sortent beaucoup mieux que les gens non socialisés. Ils peuvent demander de l'aide à leur entourage pour comprendre ou faire quelque chose[60] »*.

Imaginaires, représentations, expériences individuelles et culture du risque

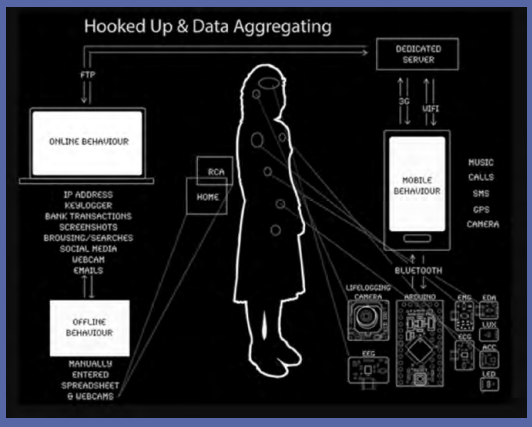
Parvenir à penser les aspects lointains, dans le temps ou dans l'espace, des enjeux et des pratiques individuelles nécessite de s'inscrire dans le temps long, de prévoir et d'anticiper les usages néfastes de nos données personnelles et, alors, de répondre aux attentes de la prévention. Or, il est particulièrement difficile de percevoir l'importance de se protéger face à des risques qui restent intangibles dans une large mesure.

Les croyances, les représentations symboliques ou les structures culturelles, variables selon les contextes nationaux et les groupes sociaux, pèsent sur la capacité des individus à attribuer du sens et à s'approprier les discours de prévention. Les significations associées à la vie privée sont multiples selon les individus et les contextes sociaux dans lesquels ils évoluent. Nous n'avons pas tous les mêmes idées, les mêmes représentations au sujet de ce qu'est la vie privée, et pas les mêmes réponses quand il s'agit de la préserver. Schématiquement, nous pouvons identifier deux grands imaginaires opposés en matière de protection des données par les individus : « Je n'ai rien à cacher » versus « Ça me fait peur ».

« Je n'ai rien à cacher ». Ce discours est fréquemment entendu chez les individus peu soucieux de la protection de leurs données personnelles. S'il témoigne d'une connaissance des pratiques de surveillance, celle-ci ne semble pas concerner les individus, notamment par méconnaissance ou absence de caractère tangible des risques. Ce discours est renforcé par l'imaginaire de « l'inévitabilisme »[61], porté par les acteurs de la Silicon Valley et ancré dans nos représentations collectives, selon lequel certains inconvénients du progrès seraient inévitables. « Si vous voulez accéder à un service gratuit, il est inévitable que l'on marchande vos données personnelles. » En ne présentant pas d'alternatives, ce discours restreint les possibles politiques : les choix technologiques ne sont pas négociés car ils nous sont présentés comme inéluctables. Il imprègne également nos représentations collectives, au point que l'affirmation « Si c'est gratuit, c'est toi le produit » est intégrée dans le comportement de certains individus, qui estiment juste que leurs données soient collectées en échange d'un service gratuit ou meilleur. À l'inverse, la complexité de l'environnement numérique suscite de nombreuses appréhensions. Le sentiment de manquer de compétences techniques pour le maîtriser alimente une réelle méfiance vis-à-vis des outils. Chez les publics en situation de précarité numérique,

58 Irène Bastard, « Quand un réseau confirme une place sociale. L'usage de Facebook par des adolescents de milieu populaire », *Réseaux*, 2018/2-3 (n° 208-209), p. 121-145.
59 Lors d'un entretien avec le LINC, 1er octobre 2020
60 Lors d'un entretien avec le LINC, 4 mars 2020
61 Shoshana Zuboff, *L'Âge du capitalisme de surveillance*, Editions Zulma, 2020

FRAGMENT D'IMAGINAIRES



« L'artiste Jennifer Lynn Morone "est parvenue au prochain stade inévitable de développement du capitalisme en devenant une entreprise. Ce modèle vous permet de tirer profit de votre santé, votre génome, votre personnalité, vos capacités, expériences, potentiels, vices et vertus". Autrement dit, la racine de la numérisation du monde (sous sa forme présente) serait d'abord sa marchandisation. »

Voir le tiré à part : https://linc.cnil.fr/vp2030

la question de la vie privée et le rapport aux données personnelles est une justification centrale à leur non-pratique comme le souligne Benjamin Bitane, responsable des formations chez Emmaüs Connect : *« Il y a une grosse appréhension et des craintes parce que c'est un milieu qu'ils ne connaissent pas. On entend souvent des personnes nous dire : "si j'utilise le numérique, ils vont connaître où j'habite, mon numéro de carte bleue, etc." Ils ont l'impression que les gens vont entrer par effraction chez eux s'ils utilisent Internet »*[62]. Les seniors en particulier ont une forte appréhension du numérique, notamment par crainte de mal faire, de divulguer des informations personnelles ou de se faire arnaquer. Ils sont donc dans une stratégie d'évitement, notamment pour tout ce qui a trait à l'argent ou aux démarches administratives. Benjamin Bitane poursuit : *« Ils peuvent utiliser fréquemment Internet, mais dès qu'il faut faire un achat en ligne ou payer ses impôts, ils vont voir des travailleurs sociaux ou des médiateurs numériques. "Je le fais avec un pro, pas parce que je n'ai pas la compétence, mais par crainte" ».* Certains refusent ainsi d'effectuer certaines démarches en ligne par crainte de divulgation non souhaitée d'informations personnelles.

Par ailleurs, les expériences individuelles influent sur la perception individuelle de la protection des données personnelles et la norme de prévoyance. Dans une enquête auprès de personnes victimes de violation de données, Dominique Boullier et Maxime Crépel soulignent que cette expérience a conduit ces individus à modifier sensiblement leurs pratiques[63]. Avant la violation, ils n'avaient pas ou peu conscience du risque. Ils ne savent en outre pas quand cette violation s'est produite, ni pour quelles raisons. Cette incertitude provoque un sentiment d'anxiété. Leur première réaction est souvent de s'attribuer la responsabilité de la faute. La majorité d'entre eux sont ensuite plus vigilants et changent leurs pratiques : mots de passe plus complexes, cache-webcam, nettoyage du cache internet, adblocks, etc. Stéphane Koukoui, médiateur numérique, corrobore ce point : *« Quand on a eu une mauvaise expérience, on est davantage vigilant. Il faut se tromper une ou plusieurs fois avant de faire attention*[64] *».* Avoir été victime fait prendre conscience du risque de piratage de ses données personnelles et rend plus sensible aux messages de prévention.

***

La protection des données gagne à être considérée du point de vue de ses publics, de l'adhésion, de la résistance ou de l'indifférence que ces messages de prévention suscitent. Elle doit être interrogée du point de vue plus transversal des inégalités et des hiérarchies sociales. Tout le monde n'est pas affecté de la même manière, n'a pas accès aux mêmes informations, n'a pas les mêmes ressources ou capacités à gérer ses conséquences. À partir de cette perspective, il est souhaitable de porter une attention et un message différent à certaines personnes, certains groupes sociaux, selon leurs vulnérabilités particulières.

62 Lors d'un entretien avec le LINC, 12 mars 2020
63 Dominique Boullier et Maxime Crépel, « Insurance for building Trust and Enabling Big Data », Joint Research Initiative – Axa Research Fund, 2015/2017
64 Lors d'un entretien avec le LINC, 13 octobre 2020

Zoom sur…

Dématérialisation des services publics, exclusion et injonction à l'exposition de soi

La dématérialisation des services publics, tout en étant un vecteur de simplification administrative et d'accessibilité plébiscité par un grand nombre d'usagers, produit dans le même temps de nouvelles formes d'exclusion et complexifie l'accès aux droits pour les personnes les plus précaires et les moins numériquement compétents. Les citoyens doivent désormais avoir recours à des outils numériques, qu'ils ne maîtrisent pas toujours pour accéder à leurs droits sociaux, à l'emploi ou à tout type de services.

Comme le rappelle Benoît Vallauri, responsable du Ti Lab Bretagne, *« Plus vous êtes précaire, plus vous êtes confronté à la dématérialisation »*[65]. Alors que les plus aisés n'ont que de rares besoins d'y avoir recours, pour payer leurs impôts par exemple, les moins favorisés doivent souvent faire face aux services numériques. Les demandeurs d'emploi doivent se réactualiser tous les mois, d'autres doivent effectuer des demandes dématérialisées pour le Revenu de solidarité active, la Couverture maladie universelle, la formation, etc. Face à la machine et à des interfaces qu'ils ne maîtrisent pas toujours, les personnes les plus précaires sont confrontées à la nécessité du dévoilement de soi, et pour certains ont de plus en plus l'obligation de se faire accompagner non plus seulement socialement, mais numériquement.

Concernant la protection des données, on peut observer chez certains une forme de méconnaissance du sujet ou de désintérêt. *« La question des données personnelles n'est jamais une problématique, les gens veulent accéder à leurs droits sociaux, ils se soucient peu de savoir qui a accès à leurs données »* constate Benjamin Bitane d'Emmaüs Connect[66]. Toutefois, Benoît Vallauri[67] pointe un différentiel de confiance entre les données à partager pour des démarches administratives et celles partagées au quotidien sur réseaux sociaux, avec une méfiance plus forte de l'administration que des plateformes. En effet, comme l'explique Héléna Revil[68], le problème ne porte pas tant sur les informations transmises que l'assignation identitaire qu'elle implique. *« Lorsque l'on donne ses informations personnelles, on rentre en quelque sorte dans un moule, dans une catégorie administrative, et l'on devient défini par ses données. »* Une personne pourra alors avoir la sensation d'endosser la stigmatisation associée à certaines identités sociales, *« ce que l'on dit sur les personnes au RSA »*, ou la *« matérialisation du handicap »*.

Benoît Vallauri relève que la perception des personnes vis-à-vis de la numérisation des formulaires produit *« le sentiment chez les personnes et chez les professionnels de l'action sociale que la mise en place de dispositifs est utilisée à des fins de contrôle et lutte contre fraude sociale plutôt qu'à des fins d'optimisation des demandes de droits, le sentiment que ça va être utilisé pour contrôler, mais rarement en faveur des usagers »*. Ceci se retrouve d'autant plus chez des travailleurs sociaux qui ont le sentiment d'être devenus des accompagnants de dossiers techniques d'aides au droit, alors que dans un mouvement symétrique, les médiateurs numériques doivent se transformer en accompagnateurs sociaux : *« la médiation numérique s'est confondue avec le travail social »*, avec la sensation pour les travailleurs sociaux que le numérique *« les dépossède de l'aide à la capacitation des personnes »*. Ces derniers peuvent alors transmettre leur méfiance aux personnes qu'ils accompagnent.

Du point de vue de la protection des données, et pour les populations les moins aguerries au numérique, la question peut paraître assez éloignée. Parfois les personnes n'ont même pas d'adresse email lorsqu'elles s'adressent au guichet. Et il n'est pas rare que les médiateurs qui les prennent en charge gardent leurs mots de passe dans un carnet pour leur permettre de se reconnecter lorsqu'ils se présentent à nouveau. Des pratiques repérées et qui ont déjà donné lieu à la mise en place de Aidants Connect[69], à l'incubateur de l'Agence Nationale de la Cohésion des Territoires, qui propose des outils et des ressources pour celles et ceux qui accompagnent *« régulièrement des personnes en difficulté avec le numérique dans la réalisation de démarches en ligne »*. Par ailleurs, la CNIL recommande régulièrement dans ses avis la mise en place d'alternatives au numérique pour l'accès aux droits ou aux services publics, dès lors que celui-ci est associé à la collecte de données.

65 Laura Fernandez Rodriguez, Inclusion numérique : « Plus vous êtes précaire, plus vous êtes confronté à la dématérialisation », *La Gazette des communes*, janvier 2021, https://www.lagazettedescommunes.com/716172/inclusion-numerique-plus-vous-etes-precaire-plus-vous-etes-confronte-a-la-dematerialisation/

66 Lors d'un entretien avec le LINC, 12 mars 2020

67 Lors d'un entretien avec le LINC, 2 juillet 2020

68 Lors d'un entretien avec le LINC, 24 novembre 2020.

69 https://aidantsconnect.beta.gouv.fr/

Des situations problématiques qui poussent à l'action auprès de la CNIL

« Je ne peux vivre sereinement en charriant derrière moi mon passé entier. »

Quentin Lafay, L'intrusion

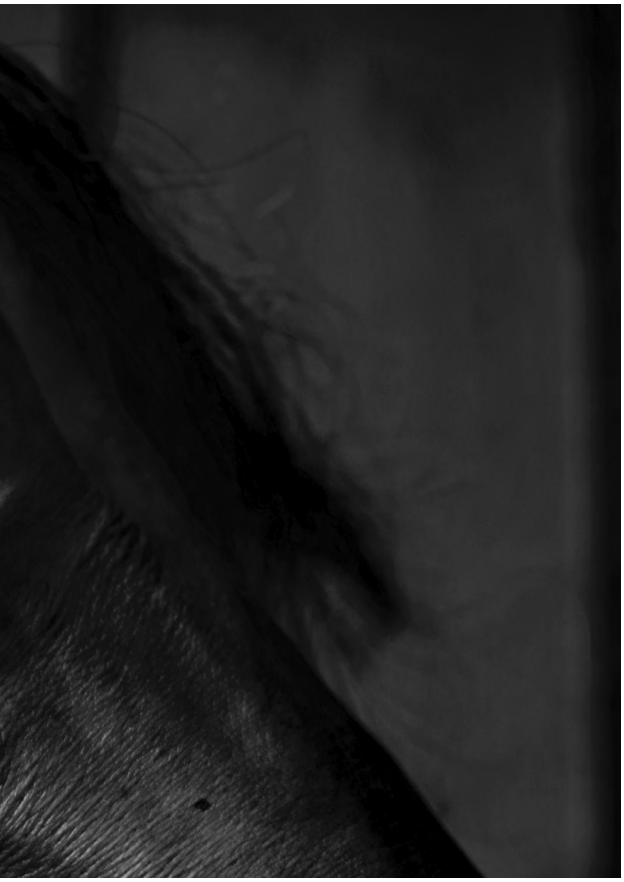
Des situations problématiques qui poussent à l'action auprès de la CNIL

Alors que les tenants du paradoxe de la vie privée *(privacy paradox)* s'interrogent sur les raisons qui poussent les individus à se dévoiler et à donner accès à leurs informations personnelles, on peut à l'inverse se demander pourquoi les individus se mobilisent (ou non) pour leurs droits relatifs à la protection de leurs données personnelles.

Pour apporter des éléments de réponse à cette question, le Laboratoire d'Innovation Numérique de la CNIL (LINC) a étudié qualitativement les courriers et plaintes reçues par la CNIL durant les mois de mai 2016 et mai 2019[70]. Les courriers rassemblés et sélectionnés contiennent des micro-récits dans lesquels le plaignant exprime sa sensibilité et relate, avec plus ou moins de détails, son expérience, les démarches entreprises, la pré-enquête qu'il a entamée, etc. Ces documents fournissent des informations sur la situation au cours de laquelle il a fait l'expérience d'une violation de ses droits[71]. Ils témoignent également de la relation entretenue avec le système de collecte et de traitement de données, des attachements dans la vie quotidienne à un système technique. Surtout, ils donnent à voir les difficultés que les individus rencontrent pour mettre en œuvre leurs droits de protection des données personnelles.

70 Le choix de ces deux dates visait à étudier une éventuelle différence liée à l'entrée en vigueur du RGPD.
En mai 2016, 689 plaintes ont été reçues par la CNIL (8,9 % des plaintes annuelles), 726 en mai 2019 (5,1 % des plaintes annuelles).

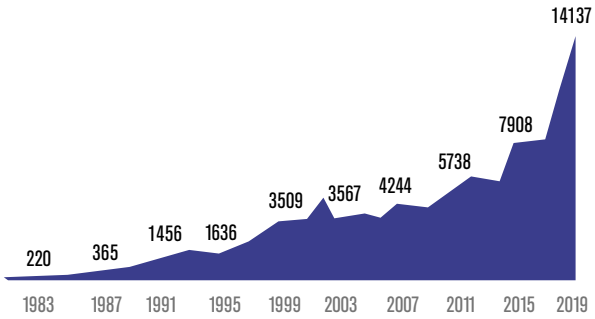
71 Le processus de mise en œuvre des droits RGPD nécessite que l'individu s'adresse dans un premier temps à l'organisme concerné, puis, s'il n'a pas obtenu satisfaction, qu'il prenne contact avec la CNIL.
Le périmètre de cette analyse est de fait limité aux situations dans lesquelles les individus ne sont pas parvenus à faire appliquer leurs droits directement auprès du responsable de traitement. Par ailleurs, certaines situations décrites dans les courriers et les plaintes échappent au périmètre de la CNIL et ne sont donc pas recevables par l'institution.



Pexels - cc-by Kat Jayne

« Les demandes que nous traitons ne sont pas liées aux caractéristiques sociales des personnes, mais aux situations qu'elles rencontrent »[72]. Cette remarque d'un chef de service de la CNIL fait écho aux travaux de la philosophe Helen Nissenbaum, pour laquelle la vie privée est toujours enracinée dans un contexte[73]. Elle rappelle que la vie privée ne doit pas être opposée au partage de l'information, mais à la diffusion inappropriée de l'information qui heurte alors ce qu'elle appelle « l'intégrité contextuelle ». Cette dernière diffère selon les normes informationnelles, les finalités, les valeurs et les intérêts propres à chaque contexte (technologique ou social). Par exemple, une même information sera aisément partagée dans une relation médicale, mais sa diffusion jugée anormale dans une situation professionnelle. Ces normes informationnelles ne se restreignent pas à ce qui est légalement possible de collecter et de diffuser. Elles incluent les valeurs politiques, les finalités de la situation, les intérêts des acteurs impliqués, la nature de leur relation, des contraintes qui s'imposent, etc. Les contours de la vie privée varient ainsi socialement et culturellement. Les plaintes et les signalements reçus par la CNIL offrent un regard sur ce que les individus considèrent comme des atteintes à « l'intégrité contextuelle », c'est-à-dire leur perception des technologies et des pratiques de collecte et de diffusion des informations comme une menace pour leur vie privée.

Nombre de plaintes reçues par la CNIL



Les premières consultations des courriers et des plaintes reçus par la CNIL surprennent par la variété des situations rencontrées et des demandes à l'institution. La seconde surprise initiale au début de cette recherche fut le faible nombre d'appels, de courriers ou de plaintes qui ciblent les grands acteurs de l'économie numérique. De même, les affaires et scandales médiatiques n'ont qu'une répercussion limitée sur les plaintes adressées à la CNIL : si les attentes envers la CNIL portent largement sur ces sujets dans le cadre des débats publics et si l'institution a, par ailleurs, une mission de vigilance et de contrôle, force est de constater que le traitement des plaintes relève d'une dynamique très distincte. En outre, la protection des données n'est pas toujours au centre de la problématique pour laquelle les individus sollicitent la CNIL : elle s'inscrit dans une situation problématique plus large pour les personnes (harcèlement commercial, usurpation d'identité, refus de crédit, conflit professionnel, etc.).

Quatre situations principales conduisent les individus à se mobiliser pour leurs droits auprès de la CNIL : quand leur réputation est menacée par des informations disponibles

72 Chef du service des droits d'accès indirect, CNIL, 3 février 2020
73 Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, 2010

en ligne, lorsqu'ils sont victimes d'intrusion dans leur sphère privée par de la prospection commerciale, en cas de surveillance sur leur lieu de travail, et enfin l'inscription dans des fichiers nationaux (accidents bancaires, antécédents judiciaires). Ces quatre situations sociales témoignent de quatre manières de concevoir la protection de la vie privée et des données personnelles.

L'ENJEU RÉPUTATIONNEL : SUPPRESSION D'INFORMATIONS EN LIGNE ET DÉRÉFÉRENCEMENT

En 2016 et en 2019, près d'un tiers des plaintes reçues par la CNIL portait sur la publication non souhaitée de données personnelles sur Internet : moteurs de recherche, réseaux sociaux, presse en ligne, etc. Ces plaintes visent à déréférencer un contenu disponible via un moteur de recherche ou à effacer des contenus publiés dans des articles de presse (retrait de l'article, anonymisation, désindexation), sur des réseaux sociaux ou des sites personnels. Elles témoignent d'une préoccupation des individus pour leur identité numérique et un souci de préserver leur réputation. Ces situations s'inscrivent dans une conception libérale de la protection des données : le droit pour un individu de contrôler la circulation des informations le concernant.

Veuillez ne plus faire apparaître mes coordonnées dans les moteurs de recherche. C'est inadmissible !! Je ne trouve pas normal que mes coordonnées puissent apparaître de la sorte sur Internet.

(Lettre manuscrite, mai 2016)

Ces plaintes concernent en premier lieu la volonté de supprimer des informations publiées à leur insu sur des sites internet ou des réseaux sociaux, par des proches ou des inconnus. Plusieurs situations entrent dans cette catégorie où le type d'information publié varie : adresse postale du domicile ou numéro de téléphone disponible sur des annuaires en ligne, photos intimes publiées sur des réseaux sociaux, commentaires déposés par des clients, des patients ou des parents, suppression de la photographie du domicile sur Google Street View, actes de dénigrement contenus sur des blogs, etc.

Cette URL concerne un pan de mon ancienne vie, j'avais déjà demandé la suppression définitive de cet article qui peut me porter préjudice dans ma nouvelle vie professionnelle, merci de supprimer cet article rapidement et définitivement. J'ai été jugé et condamné, j'ai refait ma vie à plus de 300 kms.

(Plainte, mai 2016)

La publication de ces informations sur internet porte atteinte à ma réputation et à ma réinsertion sociale et professionnelle (recherche de logement, de travail, etc.). En effet, n'importe qui peut accéder à mon passé judiciaire alors que j'ai été jugé et ai payé ma dette à la société. Aujourd'hui, j'ai pour objectif de me réintégrer dans la société, de retrouver une vie normale et ce type d'article ne m'aide en aucun cas dans mes démarches.

(Lettre, mai 2019)

Le second motif de demandes est lié au déréférencement de certains contenus anciens ou erronés associés à l'identité patronymique des individus, et, qui nuisent à leur réputation. Ces demandes sont souvent liées à des décisions de justice anciennes, ou invalidées par la suite, telles qu'une personne ayant été mise en examen avant d'obtenir un non-lieu. Les individus doivent s'adresser d'abord aux moteurs de recherche, puis solliciter la CNIL s'ils n'obtiennent pas satisfaction. En France, Google indique avoir reçu près de 225 000 demandes de suppression de résultats de recherche depuis l'entrée en application du droit au déréférencement en mai 2014[74].

Ces demandes de suppression d'informations ou de déréférencement sont révélatrices des enjeux pour la vie privée liés aux caractéristiques des espaces publics en réseau, qui compliquent les manières de protéger sa vie privée, en rendant les individus plus vulnérables à un « effondrement de contexte », comme nous le décrivons dans la partie 2 (page16). L'indexation par les moteurs de recherche des traces laissées par (ou sur) les individus et leur association à leur identité civile déplacent les frontières public/privé. Dans la grille d'analyse liée à « l'intégrité contextuelle » décrite ci-dessus, la publication d'informations personnelles en ligne, c'est-à-dire disponibles pour n'importe quelle utilisation par n'importe qui, apparaît comme la forme la plus extrême de « décontextualisation », porteuse des plus grands risques pour les personnes. Par exemple, cet individu devenu surveillant pénitencier, souhaite que soient supprimées les informations le concernant pour cloisonner ces différentes sphères sociales, et ainsi protéger sa famille.

74 Google, Rapport de Transparence, *Demandes de suppression de contenu dans le cadre de la législation européenne sur le respect de la vie privée*, https://transparencyreport.google.com/eu-privacy/overview

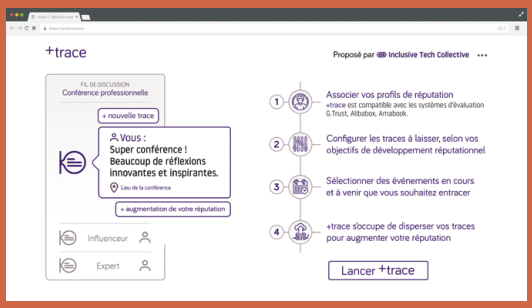
Je me permets de vous solliciter afin que vous procédiez sans délai à la fermeture des pages où mon nom apparaît, pour des raisons de protection. En effet, je suis dans une nouvelle orientation professionnelle, surveillant dans l'administration pénitentiaire, ce qui m'oblige à me protéger vis-à-vis d'internet et des moteurs de recherche aussi bien pour moi que pour le bien être de ma famille.

(Lettre, mai 2016)

Ces demandes témoignent d'une sensibilité des individus pour la protection de leur vie privée et l'exposition de soi. S'ils ne disposent pas nécessairement des compétences pour construire leurs identités numériques, par leurs recherches sur des moteurs de recherche, ils veillent à ce que les informations les concernant ne nuisent pas à leur réputation. À ce titre, ils cherchent à définir leur représentation de soi en ligne et à maîtriser les frontières entre leurs différentes sphères sociales. Ces pratiques soulignent que les individus ne sont pas passifs vis-à-vis de leur vie privée. Ils sont au contraire inscrits dans des pratiques réflexives pour définir et gérer leurs identités, personnelle et sociale, en maîtrisant ce qui est visible ou non (page 16). Cela semble devenir particulièrement indispensable à l'heure où le capital réputationnel devient un enjeu majeur dans des contextes de plus forte concurrence sur les marchés professionnels ou matrimoniaux[75], où les statuts sociaux sont fragilisés. Les plaignants mentionnent très souvent l'importance de leur identité en ligne pour préserver leur réputation (ou à l'inverse que l'atteinte à leur vie privée est une atteinte à leur réputation).

FUTUR SPÉCULATIF

Réputé ou répudié



En 2032, la réputation figure en bonne place parmi les métriques qui conditionnent la vie quotidienne. La notation ubiquitaire et continue a fait de ce facteur social, autrefois intangible et diffus, un bien mesurable et traçable dans l'espace et dans le temps. Somme cumulée de traces, la réputation n'est plus subjective mais bien *data-driven*.

Pour essayer de duper ce système de notation et prendre en main sa réputation, il est devenu habituel d'avoir recours à des dispositifs numériques. Appelés les « entraceurs », ces outils permettent de disséminer des fausses traces de présence à des événements pour simuler sa participation à une conférence ou un salon professionnel.

Voir le tiré à part : https://linc.cnil.fr/vp2030

L'INTRUSION DANS LA SPHÈRE PRIVÉE : LA PROSPECTION COMMERCIALE

Le second motif de plaintes concerne la prospection commerciale ou politique, qui représente 15 % des plaintes reçues par la CNIL en 2019 (33 % en 2016). Dans ces plaintes, contrairement à la situation précédente, l'atteinte à la vie privée n'est pas un dommage à la réputation individuelle, mais une intrusion dans la sphère privée. Ces situations s'inscrivent dans le prolongement de la définition historique de la vie privée et de son cadre protecteur. L'intégrité contextuelle n'est plus respectée dans la mesure où la séparation entre l'espace intime et l'espace public et commercial est brouillée.

Si tous les plaignants ne précisent pas les conséquences de ces courriers, appels ou emails non sollicités, certains décrivent le préjudice subi. Pour plusieurs d'entre eux, la situation confère au harcèlement et conduit à une atteinte psychologique.

75 En particulier au sein des classes populaires, comme le démontre Benoît Coquard qui insiste sur l'importance du capital réputationnel et du souci constant d'avoir « bonne réputation ».
Benoît Coquard, *Ceux qui restent. Faire sa vie dans les campagnes en déclin*, La Découverte, 2019

Maman est une personne âgée, invalide avec pathologies multiples, elle est harcelée par sa ligne téléphonique fixe et mobile, qui ne cesse de sonner. (…) Cela est devenu insupportable pour maman, je la retrouve épuisée en pleurs tous les soirs !!! Il faut que cela cesse, cela a un impact direct sur sa santé.

(Lettre tapée, mai 2016)

Démarchage téléphonique que nous subissons régulièrement par des individus non identifiés la plupart du temps. C'est une violation de la vie privée parce que matraquage (…) RAS LE BOL.

(Lettre manuscrite, mai 2016)

10 mails par jour, impossible de se désinscrire malgré les liens web, appel téléphonique pour me désinscrire. C'est du harcèlement qui dure depuis plus d'un an. Une honte que ces gens puissent pourrir la vie en toute impunité.

(Plainte, mai 2016)

Ces situations de prospection commerciale non désirée illustrent l'insertion des données personnelles dans de vastes et peu visibles infrastructures techniques, distribuées entre plusieurs organisations, et sur lesquelles les individus n'ont que peu de prises. La collecte des données personnelles fait problème quand cette infrastructure surgit dans la vie des gens et s'invite dans leur quotidien.

Cette société m'a démarché par mail bien que je ne lui ai jamais communiqué mon adresse email. Je lui ai donc demandé de m'indiquer quelle personne ou organisme lui avait transmis cette information mais elle n'a pas été en mesure de me répondre. J'aimerais vraiment connaitre l'origine de cette « fuite » car j'ai créé cette adresse mail expressément à titre personnel et je ne m'en sers jamais sur les sites commerciaux. Justement pour ne pas y être sollicitée !

(Plainte, mai 2016)

Je suis abonnée chez [Opérateur 1] et je reçois des appels de [Opérateur 2] pour me faire basculer chez eux. J'ai demandé à ne plus être rappelé. D'ailleurs comment ont-ils eu mes cordonnées ? Une fois, ils m'ont même réveillé un jour de repos. Autant vous dire que j'en ai marre. J'invoque la loi Informatique et Libertés à chaque fois auprès de l'interlocuteur mais rien n'y fait, ça rappelle toujours. Encore ce matin d'ailleurs. Personne n'est capable de me supprimer de leur fichier. Ras le bol

(Plainte, mai 2019)

J'ai commandé des produits sur ce site jusqu'à ce que mon chien décède. À deux reprises, lorsque je recevais des courriels publicitaires, j'ai demandé à me désinscrire par le lien de bas de page. Sans succès. Hier j'ai encore reçu un courrier, et le lien de désinscription ne fonctionnait pas. Aujourd'hui, ça recommence, et j'ai essayé de leur envoyer directement un courriel, par le biais du formulaire de contact de leur site. Mais pour pouvoir leur envoyer un courriel, il faut non seulement accepter les CGV, mais également accepter de recevoir des messages publicitaires ! Je ne sais plus quoi faire !

(Plainte, mai 2016)

Face à ces situations, les individus saisissent la CNIL quand ces appels leur portent préjudice et qu'ils ne parviennent pas à les faire cesser[76]. Ils manifestent ainsi un sentiment d'absence de contrôle, voire de panique, face à l'impossibilité de se désinscrire de ces listings. Le cas du spam témoigne des difficultés à faire exercer ses droits face à une infrastructure complexe, au sein de laquelle la chaîne de la donnée est longue. Il est difficile pour les individus isolés de comprendre le fonctionnement de ce marché opaque qu'est celui de leurs données personnelles mobilisées pour la prospection commerciale, tout comme pour les entreprises qui utilisent ces informations qui se retrouvent parfois sans prise sur cette infrastructure.

76 Ces sollicitations commerciales peuvent par ailleurs être sanctionnées par la répression des fraudes pour démarchage agressif. De nombreuses plaintes « échappent » ainsi à la CNIL et sont déposées auprès de la répression des fraudes ou du médiateur de l'énergie. Voir par exemple :
https://www.lemonde.fr/economie/article/2020/09/15/energie-enquete-sur-le-demarchage-telephonique-mensonger_6052194_3234.html

Zoom sur…

Les arnaques : intrusion dans la sphère privée et recherche de l'attention

Comme l'analyse Finn Brunton en retraçant l'histoire du spam, ces activités indésirables, qui prennent des formes multiples et qui s'insèrent dans les interstices des réseaux, ont pour point commun de chercher à capter l'attention des individus *« comme un butin dont il faut s'emparer »*[77]. Cette intrusion dans la sphère privée de l'individu pour rechercher son attention poursuit des finalités diverses, et plus ou moins légitimes selon l'expéditeur, le medium ou la nature du message : commerciales, politiques ou criminelles.

Cette volonté de capter l'attention de l'individu nous conduit en effet à inclure dans cette catégorie de plaintes les doléances reçues dénonçant les arnaques en ligne, même si elles dépassent le périmètre de compétence de la CNIL. Certaines d'entre elles fonctionnent sur ce principe d'intrusion dans la vie privée des individus (par envoi d'emails ou de courriers), afin de capter leur attention et de les hameçonner en profitant de leur crédulité. Plusieurs types d'escroqueries via spam peuvent être identifiés[78].

À cet égard, les arnaques à la webcam témoignent de ce couple intrusion / attention : les escrocs jouent sur les sentiments de honte et de culpabilité de l'individu et le menacent de nuire à sa réputation en dévoilant des informations compromettantes qu'ils indiquent avoir captées via la caméra intégrée de l'ordinateur.

Pour se protéger face à ces spams, les personnes doivent se doter de dispositifs techniques anti-spam[79] et développer des compétences individuelles : reconnaître les adresses frauduleuses en sachant lire un en-tête d'email, identifier les messages trompeurs, etc. Or, les utilisateurs moins aguerris d'Internet, qui ont recours à ces technologies essentiellement à des fins pratiques (payer ses impôts, échanger avec sa famille restée à distance, réserver un billet de train, accéder à ses comptes, exercer son activité professionnelle, etc.) maîtrisent moins ces outils et sont moins vigilants face aux techniques mobilisées par les escrocs pour capter leur attention.

Comme le décrit Nicolas Auray, ces derniers mettent en œuvre des techniques pour susciter les émotions du récepteur : appel à des valeurs partagées (générosité, sollicitude), promesses exceptionnelles (gains financiers, relations amoureuses, meilleure santé, etc.), menaces (révélations d'informations compromettantes, mises en demeure de paiement, poursuites judiciaires) tout en se parant des attributs de sérieux (jouer sur l'apparence et la similarité avec les sites officiels) et se coulant dans une familiarité de pratiques pour tromper la capacité de discernement de la victime. Ces novices constituent des cibles de choix pour ces criminels qui entendent profiter de leur crédulité.

À ce titre, les appels reçus par la CNIL durant la crise du Covid-19 témoignent de la détresse d'une partie de la population face à ces technologies numériques qu'ils ne maîtrisent pas.[80]

77 Finn Brunton, « Une histoire du spam. Le revers de la communauté en ligne », *Réseaux*, vol. 197-198, no. 3-4, 2016, pp. 33-67. https://www.cairn.info/revue-reseaux-2016-3-page-33.htm

78 Nicolas Auray en identifie trois : des spams à but commercial (visant l'achat de produits), des escroqueries à la loterie (miroitant une forte somme en échange d'un paiement initial), des « romance scams » (escroqueries à l'amour et au chantage affectif). Nicolas Auray, « Manipulation à distance et fascination curieuse. Les pièges liés au spam », *Réseaux*, vol. 171, no. 1, 2012, pp. 103-132. https://www.cairn.info/revue-reseaux-2012-1-page-103.htm

79 Nicolas Auray (op. cit.) analyse les techniques mises en place par les spammeurs pour déjouer ces dispositifs techniques.

80 https://www.cnil.fr/sites/default/files/atoms/files/rapport_cnil_point-etape_covid-19.pdf

PANOPTIQUE ET ENTRAVE AUX LIBERTÉS : LA SURVEILLANCE AU TRAVAIL

La surveillance est l'activité consistant à enregistrer et traiter des activités d'individus ou de groupes dans le but de vérifier l'adéquation des comportements à une norme sociale préétablie. Dans cette optique, l'entreprise est une figure traditionnelle de la surveillance aux côtés de la surveillance marchande et étatique. Elle s'exerce dans le cadre de relations sociales asymétriques, où la hiérarchie entend exercer une surveillance latente, ou une supervision de l'activité, à des degrés divers, pour les besoins du management. Les techniques de surveillance ont évolué parallèlement aux technologies offertes et aux modalités d'organisation du travail privilégiées. Vigiles, contremaîtres et cadres contrôlent l'activité par une présence physique sur les lieux de travail ou l'analyse des rendements et des qualités. Puis, les systèmes automatiques de badges se sont substitués au contrôleur humain. Enfin, la vidéosurveillance et la géolocalisation sont venus compléter cet arsenal de surveillance sur les lieux de travail. Ces dernières sont les deux motifs principaux de plaintes concernant la surveillance au travail.

La surveillance des employés représente 10,7 % des plaintes reçues en 2019 par la CNIL (14 % en 2016). Les raisons invoquées pour mettre en place les dispositifs de surveillance sont essentiellement des questions de sécurité. Toutefois, les finalités du dispositif sont parfois détournées de ces finalités déclarées pour contrôler l'activité des salariés[81]. Or, pour être légales, ces mesures doivent être proportionnées, et en aucun cas la surveillance ne peut être constante et permanente. La vidéosurveillance concentre le plus de plaintes, en particulier lorsque les caméras filment les postes de travail ou les lieux de pause ou sont consultables à distance. Les salariés dénoncent à la fois le manque d'information préalable à la mise en place des caméras, l'orientation de celles-ci sur leurs activités et leur usage à des fins de management par leurs employeurs.

> *On m'avait dit [que les caméras] ne servaient que pour la sécurité et non pour nous espionner et nous donner des ordres ou remarques désobligeantes.*
>
> **(Plainte, mai 2016)**

> *Une caméra est installée et observe tous nos faits et gestes. […] Cela joue sur mon moral et mon envie d'aller au travail*
>
> **(Plainte, mai 2016)**

> *La gérante a installé au-dessus de mon poste de travail une caméra de vidéo-surveillance qui filme et enregistre tous mes faits et gestes. Je suis très gêné par ce système, et je ne peux aborder le sujet sans que la gérante ne se braque et me dit « c'est comme cela et pas autrement ». Suis-je obligé de subir cette surveillance permanente ? Étant donné que je suis le seul salarié, je ne peux rien dire et me retrouve au pied du mur.*
>
> **(Plainte, mai 2016)**

Si la surveillance est en réalité discontinue, les salariés ont le sentiment d'être constamment surveillés. Que la surveillance soit ou non avérée, la seule présence de caméra suffit à conditionner le comportement individuel des salariés. À ce titre, elle est un puissant mécanisme de contrôle qui conduit les individus à se conformer à ce qu'ils pensent être les normes et les attentes de leur employeur. Au-delà du sentiment diffus de surveillance, nombre de plaintes témoignent de l'usage de ces dispositifs pour contrôler et réprimander les comportements des salariés.

> *Je me permets de vous écrire suite à plusieurs actions de mon employeur à mon encontre. J'ai reçu un sms me signalant ma vitesse excessive. J'ai été contrôlé en dehors de mes horaires de travail. [alors qu'il passait un entretien dans une autre société] Je ne peux jamais désactiver la géolocalisation de mon véhicule.*
>
> **(Plainte, mai 2016)**

> *Mon employeur a récemment installé un système de vidéosurveillance (4 caméras) dans notre commerce dont plusieurs nous filment directement en continu. Ce système permet à notre employeur de nous observer en temps réel à partir de chez lui ou de son smartphone, ce qui lui permet de nous appeler pour nous donner des ordres à distance en fonction de ce qu'il a pu observer.*
>
> **(Plainte, mai 2016)**

81 https://www.cnil.fr/fr/la-videosurveillance-videoprotection-au-travail

Le nombre de plaintes pour surveillance sur les lieux de travail est à mettre au regard de l'accessibilité de ces dispositifs techniques. Les caméras de vidéosurveillance et les dispositifs de géolocalisation des véhicules sont dorénavant disponibles à des coûts abordables facilitant leur usage par des entreprises de petite taille. Cette surveillance s'inscrit également dans l'évolution des modes de management au travail.

Les relations hiérarchiques se sont transformées pour privilégier une vision de la subordination comme « intégration dans une organisation » plutôt que comme « soumission aux ordres d'un chef ». Plutôt que l'autorité directe, les salariés sont invités à faire preuve d'autonomie dans l'organisation du travail. « *Une forme nouvelle de subordination qui se donne à voir : celle de l'allégeance. Le lien d'allégeance inféode une personne aux objectifs d'une autre, qui tout à la fois la contrôle et lui concède une certaine autonomie et une certaine protection. Ce nouveau paradigme rend compte aussi bien des nouvelles formes de relations individuelles de travail (salarié ou non) que des nouvelles formes d'organisation des entreprises (en chaînes de production et en réseaux)* »[82].

Si le contrôle de cette autonomie par les managers n'est pas illégitime, il doit être proportionné et loyal, a fortiori quand il est exercé à l'aide d'outils technologiques traitant des données (images, déplacements) qui dépassent l'enregistrement de la stricte activité professionnelle. Or, le manque d'informations et de transparence des dispositifs de surveillance témoigne plutôt d'une relation de défiance dans le cadre professionnel.

Ce manque de confiance envers les employés est accru lorsque le travail est effectué à distance, ce que souligne notamment le recours à de nouveaux dispositifs de surveillance mis en place par les employeurs lors de la crise sanitaire (keyloggers, etc.).[83]

Dans le cadre professionnel qui constitue la source de subsistance des personnes, la surveillance, dont les modalités tendent de plus en plus à recouvrir aussi la sphère non professionnelle, privée voire intime, n'est plus la simple vérification de l'exécution des tâches mais agit comme un mécanisme de contrôle des individus en tant que personnes.

LA SURVEILLANCE INSTITUTIONNELLE ET LES EXCÈS BUREAUCRATIQUES : LE FICHAGE INFORMATISÉ

La quatrième catégorie principale de situations conduisant les individus à solliciter la CNIL pour exercer leurs droits concerne le fichage informatique. Ces cas témoignent de situations où les individus ne sont pas informés de leur inscription dans des fichiers informatiques et le découvrent (ou le suspectent) de manière fortuite. Les fichiers d'incidents de la Banque de France sont l'objet de multiples appels, courriers et plaintes (plus de 400 plaintes en 2019, plus de 500 en 2018), notamment le fichier d'incidents de remboursement des crédits aux particuliers (FICP) et le fichier central des chèques (FCC).

Les plaintes concernent plus spécifiquement des contestations d'inscription ou le maintien de l'inscription des personnes alors qu'elles ont régularisé leur situation. Dans la majorité des cas, il s'agit de défaut de procédures au sein des établissements de crédit (révélant la dimension humaine de la chaîne de la donnée). Or, ceux-ci restreignent les capacités des individus à contracter un nouveau crédit.

> *Le fichage actuel est donc à la fois abusif et illégal, la dette n'existant plus, j'en suis arrivée à cette situation suite à un divorce douloureux et difficile. Aujourd'hui, j'ai retrouvé un emploi stable, salariée en cdi malgré mes 59 ans mais le fait d'être fichée FICP me pose beaucoup de problèmes et m'empêche d'avancer et de me reconstruire.*
>
> **(Lettre, mai 2016)**

> *Ma vie est très impactée par cette situation. Je me vois refusée par le premier conseiller financier qui daigne me recevoir. Une grande pression psychologique pèse sur moi car je ne peux envisager aucun projet dans la situation actuelle.*
>
> **(Lettre manuscrite, mai 2016)**

82 Alain Supiot, *Le droit du travail.* Presses Universitaires de France, 2016

83 La CNIL a publié en novembre 2020 une FAQ relative aux droits des salariés en télétravail, https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail

Les plaignants témoignent des difficultés à faire reconnaître leur statut de victimes auprès des banques et institutions financières (alors qu'elles étaient considérées comme coupables préalablement d'accident de paiement). La dénonciation auprès de la CNIL apparaît dans ce cas de figure comme un moyen pour 1) se voir reconnaître son statut de victime 2) faire pression sur la banque. Pour cela, leurs justifications sont à la fois factuelles et morales. Ils relatent les faits en mentionnant l'ancienneté de leurs problèmes financiers et la régularisation de leur situation. Surtout, tous ajoutent à cette présentation factuelle des valeurs morales pour s'indigner de leur inscription dans ces fichiers comme le précise une téléconseillère de la CNIL : *« Beaucoup ressentent également le besoin de nous dire qu'ils sont très honnêtes. Qu'ils sont dans leur bonne foi, qu'ils ne sont pas mauvais payeurs, etc. Il y a un enjeu moral également d'une situation qu'ils jugent injustes par rapport à leurs valeurs personnelles ».*

J'ai malheureusement été fiché à la suite du dépassement du découvert autorisé de quelques euros. Le fichage a été effectif sans que j'en sois tenu au courant et étant actuellement dans une démarche de recherche de financement pour un projet professionnel je me suis aperçu de cette fâcheuse situation m'handicapant gravement au vue de l'urgence de ma situation. C'est d'ailleurs l'un des éventuels investisseurs qui m'a fait part de mon fichage. Aussi j'ai rapidement remédié à ce problème mais il en va autrement pour la Banque qui fait durer cette situation me causant d'énormes torts.

(Plainte, mai 2016)

J'ai malencontreusement fait un chèque de 300 euros sur un compte clos. Je ne m'en suis pas rendu compte et j'ai reçu la notification d'inscription.

(Plainte, mai 2019)

Récemment confrontée au refus d'une demande de crédit auprès de ma banque, j'apprends avec étonnement que mon nom figure au FICP. J'ai contacté la Banque de France pour en connaître l'établissement. Il s'agit de [un établissement de crédit] alors que j'ai remboursé le crédit renouvelable depuis 2016. Malgré un premier courrier envoyé en septembre 2016 puis une deuxième en juin 2018, la société n'a pas jugé utile de mon répondre.

(Plainte, mai 2019)

Ces situations relatives au fichage font écho à la mobilisation collective et aux débats des années 70 qui ont conduit à la loi Informatique et Libertés. Face à l'informatisation des services de l'État et des fichiers d'administrés, des tensions se font jour sur les données collectées, leur exploitation, leur durée de conservation, l'interconnexion des fichiers et la possibilité des individus d'intervenir sur ces données. À l'époque, la mobilisation est collective contre ces projets de fichage. Ici, la dénonciation est individuelle et vise moins la légitimité de ces fichiers que les défauts de mise à jour.

Zoom sur…

Des motifs de plaintes historiques

La prospection commerciale, la réputation, la surveillance au travail et le fichage informatisé sont des motifs récurrents de plaintes depuis la création de la CNIL. Les rapports annuels de l'institution donnent un aperçu de la constance de ces situations problématiques, malgré les modifications progressives de leurs modalités et l'apparition de nouvelles technologies et de nouveaux usages.

Depuis la création de la CNIL, **la prospection commerciale** est l'une des principales motivations de plainte. Elle figure comme la première des préoccupations mises en avant dans le premier rapport annuel : *« La Commission a été saisie à plusieurs reprises de réclamations de personnes physiques se plaignant d'être importunées par une publicité leur parvenant à leur domicile sans qu'ils l'aient voulue, et quelquefois ce qui est manifestement plus grave, au lieu de leur travail. »* Ces envois de publicité vont évoluer avec le développement technologique : aux courriers postaux vont s'ajouter les appels téléphoniques, les télécopies, les SMS et les emails. Le spam – dont la CNIL rappelle l'origine du terme dans son 22e rapport annuel : un sketch des Monty Python – va conduire le régulateur à expérimenter en 2002 une boîte-mail permettant aux individus de transférer leurs sollicitations par mail, et à la CNIL d'en étudier les contenus et les émetteurs[84]. Cette mission est aujourd'hui assurée par l'association Signal Spam[85].

La question du levier d'action d'un **individu face au fichage**, notamment administratif, à l'origine même de l'institution, est prégnante dans les actions de la CNIL et l'un des motifs récurrents des plaintes. En dehors de la prospection commerciale, les thématiques de la banque, de la fiscalité et du crédit sont régulièrement dans les principaux motifs de plaintes de la part des particuliers. En 1985 par exemple, les *« plaintes relatives à leur inscription dans des fichiers de mauvais payeurs entraînant refus de crédit »*[86] font partie des principales causes de sollicitations par les individus.

La surveillance au travail est une thématique qui, rapidement, entraîne l'institution à intensifier ses travaux, et ce dès 1983 : *« les incidences de l'informatique sur les relations de travail, les dangers qu'un développement non maîtrisé de cette technique pourraient même comporter pour la liberté du travail ont amené la Commission à créer en son sein, une sous-commission chargée de ce secteur »*. La CNIL constate, dans son rapport de l'année 1987, qu'un « système » dans lequel les « personnes travaillant sous la surveillance d'une caméra » est « appelé à connaître un développement certain »[87], jusqu'à noter à partir de l'an 2000 l'émergence de la « cybersurveillance des salariés ».

Enfin, **l'enjeu réputationnel**, lié notamment à la question de la publicité d'informations dans des journaux (voir partie 1 page 30), prend une importance accrue avec l'avènement d'Internet et de la conservation des données en ligne après leur indexation sur un moteur de recherche. La CNIL évoque en 1997 à titre illustratif le risque d'informations conservées dans les « newsgroups »[88], pouvant être récupérées aisément via un moteur de recherche – et plus encore en 2012 quand s'est démocratisé le système de « tag » des photographies, ajoutant l'image à l'information. Le droit au déréférencement, en déclinant opérationnellement les droits d'opposition et de suppression de la loi Informatiques et Libertés de 1978 au système de fonctionnement particulier des moteurs de recherche, relance la visibilité de cette question de la maîtrise des informations en ligne à partir de 2014.

84 « En l'espace de trois mois, environ 325 000 « spams » ont été reçus ce qui démontre la mobilisation qu'a suscitée l'opération « boîte à spams », les internautes trouvant enfin un relais institutionnel au problème du « spamming » face auquel ils sont, le plus souvent, désarmés, tant d'un point de vue technique que juridique. »

85 https://www.cnil.fr/fr/spam-phishing-arnaques-signaler-pour-agir

86 Les demandes des particuliers sont de deux sortes : • réclamations relatives à des questionnaires à remplir ; • plaintes relatives à leur inscription dans des fichiers de mauvais payeurs entraînant refus de crédit.

87 La décision de la CNIL du 15 décembre 1987 fixe un certain nombre de garanties essentielles pour les personnes travaillant sous la surveillance d'une caméra, système appelé à connaître un développement certain

88 Grâce à ces moteurs de recherche de « newsgroups », il est possible à partir de l'un des messages que vous avez envoyés, de récupérer toutes les autres interventions que vous avez faites sur tous les autres « newsgroups » et ainsi d'obtenir un profil assez net de vos centres d'intérêt.

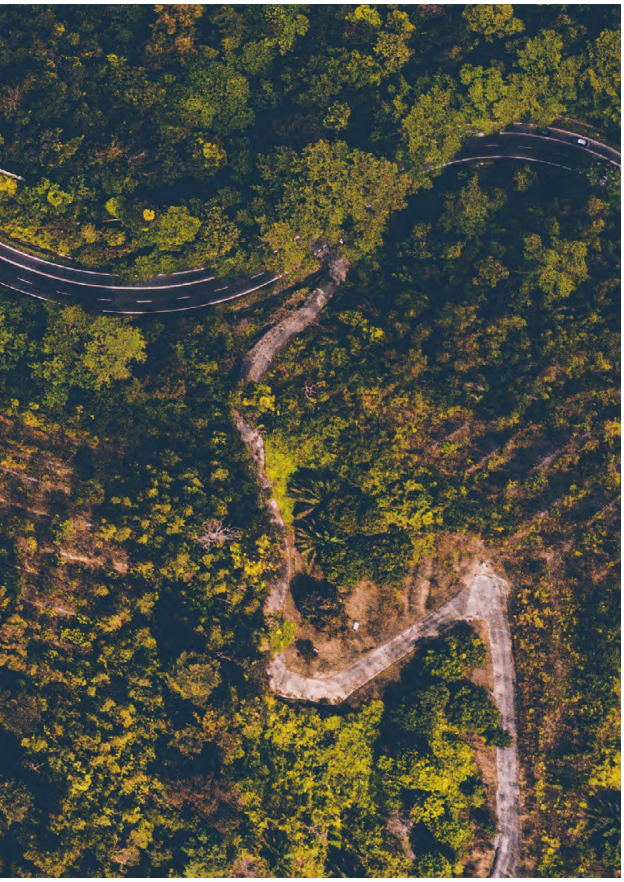
Les chemins du droit : les étapes préalables au recours à la CNIL

« On ne peut pas briser de chaînes quand il n'y en a pas de visibles »

Franz Kafka, Le Procès (1933)

Les chemins du droit : les étapes préalables au recours à la CNIL

Au-delà de la diversité de ces situations, les plaintes donnent à voir les chemins du droit empruntés par les individus, un parcours aux multiples obstacles qu'ils doivent surmonter avant de faire valoir leurs droits auprès de la CNIL.
Le recours aux droits est le fruit d'un processus incertain, au cours duquel, l'infrastructure de données doit être rendue visible, l'individu se considérer comme une victime du traitement de données, et être dans une situation sociale asymétrique qui l'empêche de résoudre le problème par lui-même.



Pexels - cc-by Deva Darshan

RENDRE VISIBLE L'INFRASTRUCTURE DE DONNÉES

L'exercice des droits nécessite de prendre conscience de la collecte et du traitement de ses informations personnelles. Or, ces opérations sont inscrites dans des infrastructures complexes faiblement visibles et compréhensibles pour l'individu. Un exemple paradigmatique de cette complexité est celui de la publicité en ligne, où, malgré le recueil du consentement par l'intermédiaire des « bandeaux cookies », l'internaute a une compréhension réduite de l'ensemble de la chaîne de la donnée et des acteurs qui y ont accès[89]. Cela nécessite de fait des connaissances à la fois sur le fonctionnement technique, sur le cadre juridique et sur l'écosystème du marché de la donnée. Surtout, les industriels tendent parfois à rendre ce fonctionnement le plus insaisissable possible pour les profanes. Leur objectif est de proposer une expérience la plus fluide possible grâce aux technologies, notamment par leur travail sur le design des interfaces[90]. Cette faible visibilité des infrastructures rend difficile la prise de conscience individuelle de l'ampleur de la collecte et du traitement de données personnelles. Quels sont les opérateurs du basculement vers la prise de conscience ?

Si les affaires médiatiques jouent un rôle de révélateur du fonctionnement de certaines entreprises, elles conduisent à peu de dépôts de plainte auprès de la CNIL. « *On reçoit peu de plaintes en réaction à l'actualité, suite à des scandales qui peuvent sortir dans la presse. (…) Cela reste marginal par rapport à l'ensemble des plaintes. On n'a pas eu par exemple de recours massif suite à l'Affaire Snowden* »[91]. Cet effet limité des affaires médiatiques sur le dépôt de plaintes s'explique en partie par le fait que ces révélations, si elles donnent à voir les dysfonctionnements et les abus dans la collecte de données personnelles, ne s'accompagnent pas d'un processus de victimation (voir infra).

> *Dès lors que je veux prendre des billets d'entrée pour une visite ou pour un spectacle par voie informatique, je dois décliner mes nom, prénom, date de naissance, adresse courriel, adresse postale, téléphone… Quand j'achète un billet au guichet, on ne me demande pas toutes ces informations. Par Internet, pour un simple billet d'entrée, est-il justifié de décliner nos coordonnées complètes ? La protection des données personnelles ne devrait-elle pas s'appliquer à ces établissements ?*
>
> **(Courrier tapé, mai 2019).**

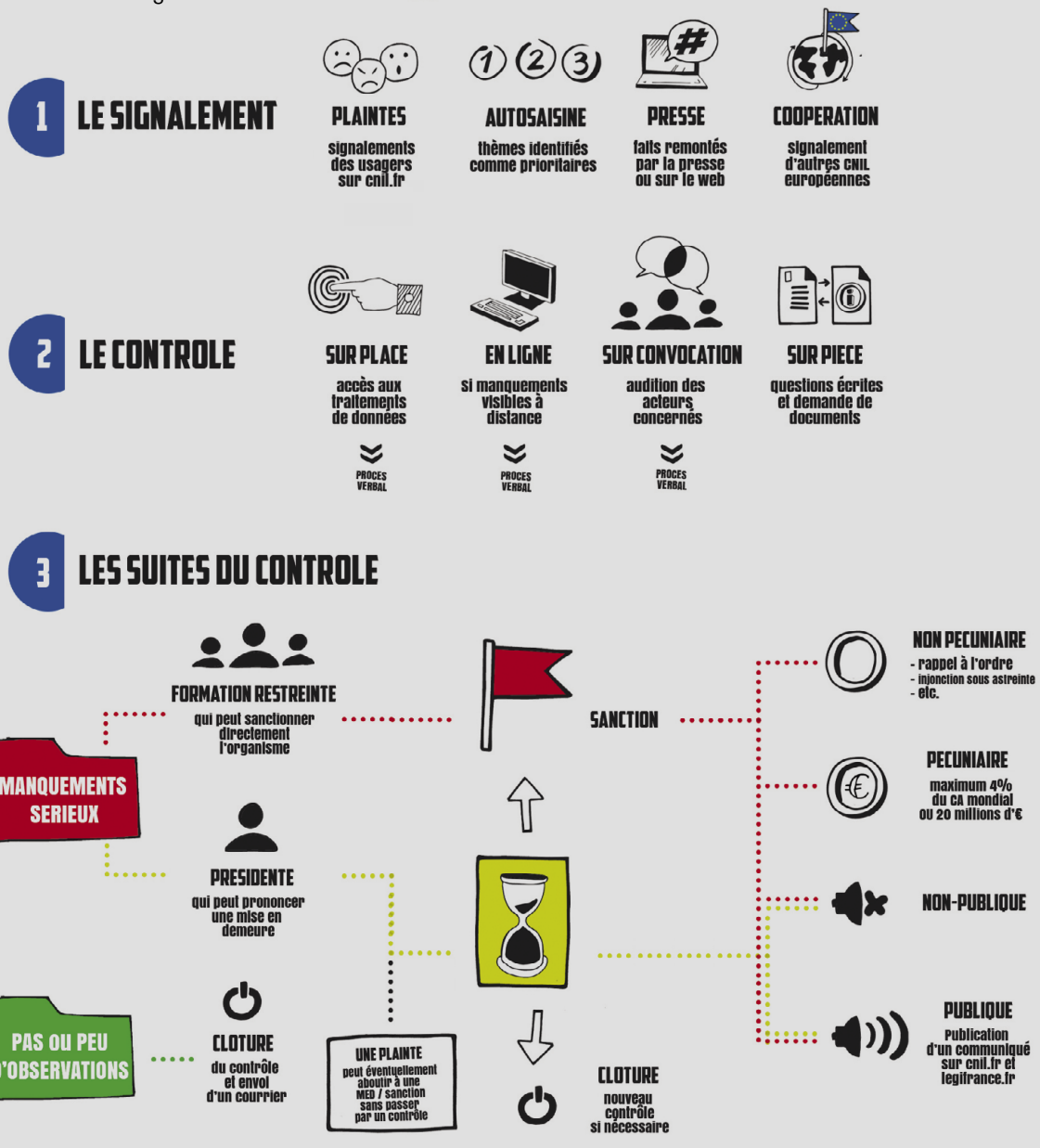
L'éveil critique sur la collecte de données se joue lors d'opérations particulières, où l'attention des individus est accrue, telles que l'inscription à un service ou un paiement en ligne, qui sont autant de moments de distension entre l'expérience fluide de la société calculée[92] et le monde sensible de l'utilisateur. Elle est également particulièrement présente lors de la recherche sur les moteurs de recherche qui facilitent la mise en visibilité des informations disponibles en ligne.

89 Voir les articles du LINC qui donnent à voir cette complexité et expliquent le fonctionnement de ces acteurs de la publicité en ligne. https://linc.cnil.fr/dossier-cookies
90 Voir le cahier IP 6 *La forme des choix*, 2019. https://linc.cnil.fr/fr/cahier-ip6-la-forme-des-choix-0
91 Entretien avec les responsables du service des plaintes, 15/01/20
92 Le terme « société calculée » désigne une société numérisée dont le fonctionnement est soumis à des calculs algorithmiques.

Zoom sur…

Les plaintes, un maillon de la chaîne répressive de la CNIL

La CNIL dispose d'une chaîne répressive complète lui permettant de recevoir des signalements par des canaux divers, dont les plaintes, puis de réaliser des contrôles. Les suites peuvent aller de la clôture, à la mise en demeure et jusqu'à la sanction, financière ou non. Dans certains cas, une publicité peut être décidée en fonction de la gravité des cas.



Les dysfonctionnements des infrastructures de données sont à l'origine de nombreuses plaintes : quand il y a une erreur, une panne, un hack de données, un « glitch » de l'algorithme, un défaut de maintenance, des emails non sollicités, une usurpation d'identité, etc.[93] La panne, loin d'être une simple rupture technique, agit comme un révélateur du réseau sociotechnique, invisibilisé en fonctionnement quotidien. L'origine de la défaillance peut être tout à la fois technique, humaine ou organisationnelle, souhaitée ou involontaire.

« Défichage impossible car problème informatique par rapport au nom marital/jeune fille. Apparemment, le compte a été formulé avec une erreur de nom. Le défichage est impossible car les noms ne correspondent pas. »

(Plainte, mai 2016)

« J'ai reçu un ticket de caisse en ligne d'achats faits chez [une enseigne de grande distribution] sur mon adresse email, alors que je n'ai pas de compte chez [cette enseigne de grande distribution] ni jamais fait d'achats chez [cette enseigne]. Après vérification, il semble que quelqu'un ait créé un compte lié à mon adresse email, mais je ne peux pas m'y connecter car ce n'est pas moi, et je refuse d'avoir mon adresse email liée à des transactions frauduleuses comme cela. »

(Plainte, mai 2019).

« Hier, nous nous sommes connectés à notre espace client [d'un établissement de crédit] pour demander des décomptes de remboursement anticipé de notre prêt à taux zéro pour juin, juillet et août 2019. Pour cela, nous avons faire plusieurs demandes et quelle ne fut pas notre surprise de nous voir transmettre pour une de ces demandes le décompte de remboursement de M. XXX, un monsieur qui nous est totalement inconnu, et pour une autre demande un mélange entre nos infos et celles de ce monsieur. Suite à cette diffusion des données personnelles, nous nous inquiétons légitimement quant à la protection de nos propres données personnelles. Comment [cet établissement de crédit] peut-il nous assurer de la protection de nos données après nous avoir transmis les données d'une tierce personne ? »

(Plainte, mai 2019)

En troublant le fonctionnement routinier des infrastructures de données, les frictions et les dysfonctionnements les rendent visibles aux individus[94]. Les défaillances de ces infrastructures sont la source d'une large part des problèmes posés par la collecte des données pour les individus. Ils sont une étape nécessaire mais non suffisante au recours aux droits. Les individus doivent également porter un jugement moral sur cette infrastructure de données et se considérer comme victime de la situation pour demander réparation.

FRAGMENT D'IMAGINAIRES

« Un immense écran public affichant un message d'erreur conduit à imaginer ce qu'il en serait si sa fonction devenait de rendre intentionnellement publiques des fuites de données ou d'autres usages abusifs. »

Voir le tiré à part : https://linc.cnil.fr/vp2030

93 À l'instar des « glitchs » algorithmiques qui révèlent le fonctionnement routinier des algorithmes.
Axel Meunier, Donato Ricci, Dominique Cardon et Maxime Crépel, « Les *glitchs*, ces moments où les algorithmes tremblent », *Techniques & Culture*, https://journals.openedition.org/tc/12594

94 À ce titre, la CNIL a recommandé à plusieurs reprises la mise en place de « frictions désirables » pour rendre visibles la collecte et le traitement de données.
Voir notamment le cahier IP *La forme des choix*, le site design.cnil.fr et le livre blanc *À votre écoute*.

SE SENTIR VICTIME DE LA SITUATION

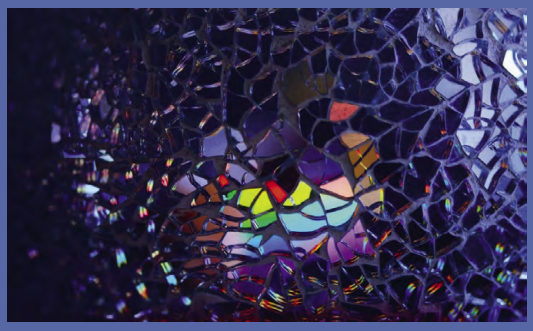
Tous les jours, des personnes rencontrent des problèmes qu'ils attribuent à la collecte ou au traitement de leurs données personnelles. Pourtant, seules une minorité d'entre elles vont se mobiliser pour faire changer la situation, alors que la grande majorité la tolère. En effet, pour qu'un individu se mobilise, le dommage doit devenir un réel préjudice : il est souvent nécessaire que la vie des individus soit *affectée* socialement, moralement, psychologiquement et/ou économiquement pour qu'ils s'estiment victimes de la situation.

Par exemple, alors que ses comptes bancaires sont approvisionnés, un couple se voit refuser trois chèques dans deux supermarchés où il a l'habitude d'effectuer des achats. Cette mésaventure leur fait prendre connaissance des systèmes de *scoring* mis en place dans ces enseignes pour identifier les chèques impayés. Ce couple s'estime victime d'un préjudice qui vient heurter ses valeurs morales. Au-delà du refus du chèque, la situation sociale dans laquelle ce dysfonctionnement se produit (un supermarché où ils ont leurs habitudes) porte atteinte à leur réputation et impacte leur image sociale.

> *Dernièrement nous avons effectué des achats dans deux magasins : 3 chèques nous ont été refusés sans motifs par ces établissements. Nous avons subi un préjudice moral car étant dans une file d'attente en caisse avec des personnes de notre connaissance. (…)*
> *Dans notre cas c'est une atteinte à nos libertés car leur critère de refus n'est basé que sur des suppositions et non sur les états des comptes bancaires auxquels ils n'ont aucun accès. Sachant que notre situation personnelle est plus que confortable et se voir refuser un chèque dans un endroit où vous êtes connu vous pose un désagrément préjudiciable.*
>
> **(Lettre tapée, mai 2019)**

Autre exemple, la diffusion non souhaitée d'une information sur Internet peut contribuer à la stigmatisation de l'individu concerné, à lui attribuer un marqueur identitaire autour duquel vont se reconfigurer, selon une modalité négative ses interactions sociales[95]. Cela peut conduire cet individu à souffrir d'un préjudice psychologique et heurter ses principes et ses valeurs morales. De même, le refus de prêt bancaire lié à une inscription erronée dans un fichier d'impayés, outre le préjudice économique, est également une offense sociale et morale vécue comme une atteinte à l'honneur des individus. En concluant leur plainte par l'expression « Vous avez régularisé votre situation et êtes toujours fiché », nombre d'entre eux témoignent que cette situation vient heurter des principes de justice légitimes dans les sociétés modernes occidentales, tel qu'un droit à une seconde chance. Ainsi, les plaintes mettent en évidence un sens moral, inscrit dans une grammaire du juste et de l'injuste, au travers de laquelle les individus interprètent la situation vécue.

FRAGMENT D'IMAGINAIRES



Équivalents numériques des street-medics, constitués pour assurer le relais des secours, les site-medics sont des bénévoles qui soignent les maux physiques et psychologiques liés à l'utilisation du numérique, non reconnus par la médecine du travail ou la sécurité sociale traditionnelle.

Voir le tiré à part : https://linc.cnil.fr/vp2030

Devenir victime nécessite de plus d'attribuer la responsabilité de cette offense vécue à un tiers. Or, de nombreuses personnes s'estiment responsables de leur situation, du fait par exemple de leur négligence quant à la diffusion d'informations personnelles ou de leur crédulité face à des arnaques. Dans les cas d'escroqueries sur Internet, Nicolas Auray relève que le sentiment de culpabilité et de honte conduit les victimes à ne pas porter plainte. Celles-ci ont souvent peur des moqueries qui pourraient leur être adressées au sein du commissariat[96].

95 E. Goffman, *Stigmate : les usages sociaux des handicaps*, Paris, 1975
96 Nicolas Auray, « Manipulation à distance et fascination curieuse. Les pièges liés au spam », *Réseaux*, vol. 171, no. 1, 2012, pp. 103-132.

« Peu de personnes viennent nous voir pour des problèmes d'usurpation d'identité, de harcèlement en ligne, ou de phishing. Elles ont un peu honte, l'impression de s'être faites avoir, d'avoir été trop naïves, d'avoir divulgué trop d'informations et qu'elles n'auraient pas dû. »[97]

Stéphane Koukoui,
médiateur numérique, Rennes

Ce sentiment de culpabilité est renforcé par la norme implicite selon laquelle la protection des données repose sur le comportement et les actes de l'individu (cf. partie 1, page 18). Les dommages subis sont dès lors interprétés comme relevant de la responsabilité personnelle. Ils sont toutefois généralement appréhendés tant par les organismes de formation au numérique (et de régulation) que par les individus eux-mêmes comme relevant des risques liés à toute pratique numérique, une conséquence secondaire difficilement évitable de notre environnement et notre économie numérique qui nous contraint à l'exposition et au dévoilement. Il est demandé aux individus d'acquérir des compétences, de mettre en œuvre des bonnes pratiques, d'adopter une « hygiène numérique », d'être précautionneux dans leur usage du numérique, etc.

Zoom sur…

Complexité de l'infrastructure, dilution des responsabilités

Le cas du spam témoigne des difficultés à faire exercer ses droits face à une infrastructure complexe, au sein de laquelle la chaîne de la donnée est longue. Il est difficile pour les individus isolés de comprendre le fonctionnement de ce marché de leurs données personnelles mobilisées pour la prospection commerciale, tout comme pour les entreprises qui utilisent ces informations et se retrouvent parfois sans prise sur cette infrastructure. Cette méconnaissance peut être volontairement entretenue par les annonceurs, mais la complexité les dépasse parfois. Certaines sociétés achètent en effet des fichiers de prospects auprès de sociétés de routage ou autres data brokers et/ou sous-traitent à ceux-ci les envois ou les appels de masse. Elles sont alors dans l'incapacité de retirer les plaignants de la base initiale qui continuent de recevoir de la publicité non souhaitée.

J'ai demandé à plusieurs reprises (la première demande date de 2014…), par téléphone ou par mail, à être retirée du fichier de [l'entreprise XX]. Malgré cela je continue à recevoir plusieurs mails par jour de leur part. J'ai eu [la directrice de l'entreprise XX] en ligne elle-même, qui m'a indiqué dans un premier temps qu'elle allait régler le problème puis en gros qu'il fallait que je contacte moi-même les sociétés auprès desquelles elle achète des fichiers. Effarant !

(Plainte, mai 2016)

Autre témoignage, publié dans Le Monde, celui d'un ingénieur spécialisé en sécurité informatique qui reçoit plusieurs appels par jour depuis plusieurs mois. Il décide de remonter la trace de son inscription dans les listes d'appel, mais se heurte à la complexité de la chaîne de la donnée. *« C'est impossible de savoir qui a vendu mon numéro : je suis sur liste rouge, j'ai appelé tous les prestataires qui ont mon numéro. Ils m'ont tous confirmé que, sur mon contrat, la case interdisant de revendre mes informations personnelles était bien cochée. Quand je demande aux opérateurs qui leur a fourni mon numéro, on me dit que c'est ERDF [l'ancien nom d'Enedis] qui a vendu mon numéro, ce qui est impossible ! »*[98].

De fait, les acteurs du démarchage s'appuient sur des listes hétérogènes, constituées d'informations éparses rassemblées ici et là : achat de listings sur des marchés de seconde main, fichiers de sociétés tierces (déménageurs, etc.), collecte de numéros sur Internet au travers de logiciels spécialisés, etc. In fine, aucun acteur de la chaîne n'est en mesure de connaître la source de l'information.

97 Lors d'un échange avec le LINC, 13 octobre 2020
98 Damien Leloup, « Démarchage dans l'énergie : un important marché de revente de fichiers clients », *Le Monde*, septembre 2020, https://www.lemonde.fr/pixels/article/2020/09/15/d-ou-viennent-les-numeros-appeles-par-les-centres-d-appel_6052211_4408996.html

Les discours de prévention à la protection des données personnelles reviennent à faire peser sur l'individu lui-même la responsabilité de sa propre protection. Ils légitiment ainsi une théorie implicite de la responsabilité qui situe le « foyer du trouble[99] » dans le comportement des individus. Les cadres interprétatifs dominants conduisent ainsi généralement l'individu à envisager son préjudice comme résultant d'une erreur de sa part. Pour recourir à ses droits, il est indispensable de redéfinir son expérience pour l'appréhender comme une situation d'injustice dont la responsabilité est attribuée à quelqu'un d'autre que soi.

Imputer cette responsabilité ne va pas de soi dans la mesure où il est parfois difficile pour l'individu d'identifier le responsable de la collecte de données. Cela a été évoqué précédemment, les infrastructures de données sont complexes et font intervenir des acteurs multiples, difficilement identifiables pour l'individu. De nombreux acteurs interviennent dans la chaîne de la donnée et pourraient, à ce titre, être considérés, par les individus, comme ayant une part de responsabilité[100]. Pour les clients victimes d'un rejet de chèque, la responsabilité doit-elle être attribuée à la chaîne de supermarché utilisant ce dispositif ? À l'entreprise développant ce système de *scoring* ? L'imputation de la responsabilité les conduit à mener une investigation pour démontrer le lien entre la collecte de données et le préjudice subi.

Enfin, le processus de victimation nécessite d'avoir conscience de ses droits. Le droit facilite la prise de conscience du tort subi, légitime le statut de victime et offre des appuis pour l'action. Cependant, la connaissance des règles de protection des données est inégalement partagée. Nombre des personnes qui sollicitent la CNIL le font pour des demandes de conseil sur leurs droits, en particulier au travers des courriers ou des permanences téléphoniques. Ils veulent lever l'incertitude juridique dans laquelle ils se trouvent (est-ce que j'ai des droits face à cette situation que je juge injuste ?) et savoir comment mettre en œuvre ces droits. Les textes de lois sont complexes, leur maîtrise par les individus est loin d'être assurée, d'autant qu'il faut parvenir à aligner leur situation particulière à une catégorie juridique abstraite.

Les professionnels du droit ou autres conseils juridiques (syndicalistes, travailleurs sociaux, fonctionnaires, etc.) aident traditionnellement les individus à traduire leurs griefs dans le langage du droit et à donner un sens général à ces cas individuels. Toutefois, peu de courriers ou de plaintes s'appuient explicitement sur le registre et les catégories juridiques. La dénonciation s'effectue généralement davantage sous l'angle moral que juridique. Les mentions au RGPD ou

Zoom sur…

La CNIL, une porte d'entrée pour les problèmes liés au numérique

« Les personnes qui nous contactent sont souvent dans une situation qu'ils jugent problématique. Ils le savent, mais ils ne savent pas comment y répondre. Il arrive aussi qu'ils nous téléphonent sans savoir vraiment si leur questionnement relève de la CNIL. D'ailleurs, beaucoup commencent leur appel en disant « Je ne sais pas si je suis au bon endroit » ou « Excusez-moi de vous déranger ». Notre rôle est de leur donner de l'info sur leurs droits, qu'ils soient relatifs à la CNIL ou non. Avec l'expérience, on est capable de les conseiller et de les orienter vers telle ou telle administration qui peut résoudre leur problème[101]. » Dotée de 6 permanences juridiques dont une permanence généraliste ouverte chaque matin, la CNIL reçoit beaucoup de questions en dehors de son champ de compétences parmi les 25 000 appels reçus par an. Elle fait office d'institution référente dans l'imaginaire de certains individus pour tous problèmes liés de près ou de loin au numérique et à Internet. *« De manière générale, les gens ne savent pas vraiment sur quoi on est compétent à la CNIL. Ils nous contactent pour tous les problèmes qu'ils rencontrent liés de près ou de loin à Internet ou à leur smartphone : cela va du cyberharcèlement sur les réseaux sociaux, aux arnaques à la webcam, à la caméra filmant la rue ou la maison du voisin, à l'usurpation d'identité, au fichage par les banques, aux cours en visioconférence des enseignants, ou encore à la surveillance de l'employeur en télétravail. Ils nous contactent aussi car ils ne savent pas toujours à qui s'adresser. On constate aussi que dans certaines situations les dispositifs de prise en charge ne sont pas complets ou même parfois balbutiants et que l'usager peut avoir jusqu'à 4 interlocuteurs de différents services publics pour un problème urgent, ce qui augmente sa situation de détresse, par exemple dans les situations de cyberharcèlement des ados[102].»*

99 Joseph Gusfield, *La culture des problèmes publics. L'alcool au volant : la production d'un ordre symbolique*, Economica, 2009, p. 51.
100 Même s'ils ne sont pas considérés comme les responsables de traitement au sens du RGPD.
101 Échange avec une télé-conseillère du service des relations avec les publics, 6 février 2020
102 Échange avec les chefs du service des relations avec les publics, 26 mai 2020

à la loi Informatique et Libertés sont rares et souvent peu précises. Ce travail de traduction juridique de l'indignation morale des individus est effectué par les agents de la CNIL, qui actent leur statut de victime en qualifiant le manquement qui constitue le préjudice et le font reconnaître auprès des organismes concernés pour faire évoluer la situation.

INVERSER LE RAPPORT DE FORCE

Au sentiment d'être victime et à la conscience de ses droits, vient s'ajouter une troisième condition pour déterminer le recours à la CNIL. Elle a trait à la distribution du pouvoir, des ressources et des contraintes propres aux situations dans lesquelles se retrouvent les plaignants. Ne parvenant pas à faire valoir leurs droits auprès de l'organisme concerné, ni à s'extraire de la situation par leurs propres moyens, les individus se tournent vers la CNIL pour inverser le rapport de force en leur faveur.

Le processus traditionnel pour faire valoir ses droits Informatique et Libertés nécessite pour eux de s'adresser directement aux organismes concernés. S'il n'est pas nécessaire de se considérer victime pour demander l'activation de ses droits, leur activation relève souvent d'un processus de victimisation. Les personnes doivent ainsi tenter préalablement de résoudre par eux-mêmes leur problème auprès de l'organisme responsable de la collecte et du traitement de données en établissant un premier contact. Dans certains cas, elles pourront mettre en place des stratégies d'évitement destinées à réduire l'emprise des sociétés en question, comme c'est le cas avec l'utilisation de bloqueurs de publicité dans les navigateurs ou en modifiant certaines de leurs pratiques (changer de réseau social ou d'itinéraire de déplacement par exemple). Si ces tentatives échouent (difficultés, absence de réponse, réponse insatisfaisante), elles pourront alors solliciter l'appui de la CNIL et sortir de l'entre soi des parties concernées. Le processus est ainsi long, tumultueux et incertain pour les individus qui se retrouvent bien souvent isolés dans un rapport de force déséquilibré, ce qui restreint leur capacité à mettre en œuvre leurs droits.

En premier lieu, ils doivent être en mesure d'identifier l'organisme responsable et d'obtenir ses coordonnées. Une démarche fastidieuse lorsqu'une ribambelle d'acteurs, formant un réseau d'intermédiaires peu lisible pour les usagers, interviennent dans le traitement de leurs données. Difficile de savoir comment son numéro de téléphone s'est retrouvé dans un listing d'appels, ou encore de déterminer l'éditeur d'un site sur lequel ils veulent faire retirer une information.

Zoom sur…

« Faire jouer la concurrence », une stratégie qui marche dans certains cas seulement

Lorsqu'un usager est insatisfait du traitement de ces données par un organisme, une stratégie consiste à arrêter d'utiliser le service en question au profit d'un concurrent perçu comme plus protecteur. Cette dynamique a été illustrée récemment à l'occasion de la modification des conditions contractuelles de Whatsapp qui a entraîné un recours à des solutions tierces comme Signal ou Telegram. Le RGPD a embrassé également cette approche avec le « droit à la portabilité » censé faciliter le changement de fournisseur en « portant » ses données d'un service à un autre. Ce droit reste toutefois méconnu et peu mis en œuvre en pratique, et sera rarement une solution si l'organisme ne répond déjà pas à l'exercice d'un droit d'opposition.

Plus largement, l'argument « concurrentiel » pourra fonctionner dans le cadre de marchés comportant peu de frictions et où les produits et services sont très homogènes et substituables entre les différents acteurs, comme le commerce de biens.

À l'inverse, quand le traitement de données est lié à un abonnement (ADSL, banque, électricité), le changement de fournisseur sera complexe, *a fortiori* pour des questions de données personnelles uniquement. De même, dans les cas de services de communication (messageries, réseaux sociaux, email, etc.), les effets de réseau peuvent rendre le changement difficile. Enfin, dans de nombreux cas, la concurrence n'existe pas, comme dans le cas de services publics ou de services en monopole ou quasi-monopole.

Le plaignant ne possède pas toutes les informations nécessaires pour connaître le responsable de son problème et lui demander réclamation.

Je souhaite faire supprimer tous mes résultats sportifs qui se retrouvent sur cette page. Le site refuse de supprimer sans que je fournisse ma carte d'identité. Sachant qu'ils utilisent déjà mes données personnelles sans mon accord je n'ai aucune confiance et ne souhaite pas divulguer de telles informations à des inconnus par mail.

(Plainte, mai 2016)

S'ils parviennent à identifier l'organisme responsable, encore doivent-ils être en mesure de faire respecter leurs droits. Certaines plaintes témoignent de l'impossibilité de faire valoir ses droits en l'absence de dispositifs (formulaires de contacts ou de modifications d'informations, adresse email, procédure non numérique) pour s'adresser à l'organisme ou lorsque les informations ont été mises en ligne plusieurs années auparavant et qu'ils ne disposent plus du mot de passe pour accéder à leur compte, cela peut aboutir à des situations kafkaïennes où pour supprimer son compte, il faut s'y connecter, ce qui est impossible lorsqu'on ne dispose plus de ses identifiants.

Je tiens à vous rappeler que je suis actuellement en détention et par conséquent je n'ai pas accès aux sites internet, je ne peux donc pas remplir de formulaires en ligne. Je souhaiterais donc avoir une autre alternative afin de remplir ces formulaires s'il vous plait, manuscrite, ce serait l'idéal.

(Lettre manuscrite, mai 2019)

Je souhaiterai supprimer un très vieux blog que j'avais étant petite. Étant donné son ancienneté, il m'est impossible de me rappeler mon mot de passe de l'époque. De même pour l'adresse mail qui y était liée. Il s'agissait d'une adresse mail @yahoo.fr mais impossible de retrouver l'identifiant ou le mot de passe. Ainsi je viens vers vous pour pouvoir supprimer ce blog, qui n'est plus en activité depuis des années.

(Plainte, mai 2016)

Ayant résilié mon abonnement chez [opérateur Internet] il y a plus de 2 ans, je ne pensais pas que mon service «page perso» était encore ouvert et avec du contenu. Ayant contacté [l'opérateur Internet] à plusieurs reprises, étant donné que cet abonnement est résilié chez eux, ils ne peuvent pas supprimer ces pages perso.

(Plainte, mai 2016)

Ces récriminations illustrent l'inscription matérielle nécessaire à l'application du droit. Les frictions à la mise en œuvre de ses droits se matérialisent également dans les exigences supplémentaires, souvent pour de bonnes raisons organisationnelles[103], mais pas toujours nécessaires, demandées par les entreprises : fournir une copie de sa pièce d'identité, adresser sa demande par courrier recommandé, etc.

Je souhaite supprimer toutes les informations du site me concernant car je ne les ai pas sollicitées et elles sont erronées. Il est tout simplement impossible de les contacter, les mails restent sans réponse ou me sont retournés.

(Plainte, mai 2016)

J'ai été cliente de [un opérateur téléphonique]. Après avoir résilié mon contrat, j'ai demandé par écrit, en suivant strictement la procédure, la suppression de toutes mes données personnelles auprès de cet opérateur. Non seulement, elles sont toujours actives sur son site Internet mais cet opérateur continue à s'en servir pour me démarcher. Tout ce qu'il a répondu à ma demande, c'est que je devais en faire une nouvelle !! Bien sûr, cet opérateur ne met aucun moyen à disposition pour être contacté et résoudre le problème...

(Plainte, mai 2016)

Je continue de recevoir des e-mails de leur part bien que je me sois désinscrite il y a quelques mois déjà. De plus, si je clique sur le lien de désinscription dans les e-mails, il est noté que je suis déjà désinscrite. Je souhaite qu'ils me suppriment réellement de leur liste de diffusion.

103 Comme s'assurer de l'identité du demandeur avant de lui transmettre des informations personnelles : voir Kashmir Hill, *Want your personal data? Hand over more please*, The New York Times, janvier 2020, https://www.nytimes.com/2020/01/15/technology/data-privacy-law-access.html

(Plainte, mai 2016)
J'ai envoyé à plusieurs reprises des demandes d'arrêt à des SMS publicitaires de la part de [l'entreprise XXX] («STOP» par retour de SMS) et je continue à recevoir très régulièrement des publicités par SMS.

(Plainte, mai 2019)

La gestion temporelle de leur demande, aux mains des organismes, est une autre illustration du rapport de force défavorable pour les plaignants face aux organismes. Un certain nombre de plaignants sont dans une situation d'urgence à laquelle ne peut faire face ce long traitement administratif de leur demande. Or, les délais de réponse sont souvent longs, de l'ordre de plusieurs semaines ou mois… quand ils existent. Le RGPD impose pourtant aux responsables de traitement une réponse « dans les meilleurs délais » et un délai maximum d'un mois, sauf complexité de la demande (article 12.3 du RGPD). Toutes ces difficultés complexifient le parcours de recours aux droits des individus, en situation d'asymétrie vis-à-vis de ces entreprises, comme le souligne le chercheur Paul-Olivier Dehaye : *« Ce ne sont pas des obstacles à minimiser. Il existe une telle asymétrie*

Zoom sur…

Des plaintes essentiellement individuelles, peu de mobilisation collective

Ce recours au droit, contrairement à ce qui est observé pour d'autres situations telles que les plaintes pour discrimination[104], est très rarement associé à un collectif (syndicats, associations, avocats, etc.) agissant comme « opérateur de médiation juridique de la plainte ». La victime intervient en son nom propre, parfois aidée par un proche (parents, enfants, etc.), les plaintes déposées par une personne morale qui prend en charge l'affaire sont marginales[105].

Cadrée par le dispositif de dépôt de plainte mis en place par la CNIL, la dénonciation est restreinte au cadre de l'interaction entre le plaignant et l'institution et ne vise pas à former un « public »[106]. Il s'agit ainsi essentiellement d'une action individuelle s'exerçant dans un cadre privé et qui vise à faire valoir ses droits et réparer un préjudice, et non une action politique qui mobilise un collectif pour défendre une cause au sein d'une arène publique au nom de valeurs collectives. L'indignation des individus s'accompagne majoritairement de la recherche d'une solution pratique pour mettre fin au problème plutôt que d'une volonté d'incriminer publiquement un acteur et de faire scandale. En d'autres termes, les personnes qui sollicitent la CNIL dans le cadre de plaintes défendent *leur* vie privée plutôt que *la* vie privée.

Le travail de montée en généralité est effectué a posteriori par la CNIL, qui agrège les cas épars en une cause collective, et engage des procédures de contrôles, qui peuvent aller jusqu'à la sanction publique.

Il existe toutefois des exceptions à ces démarches individuelles. Le RGPD a en effet introduit la possibilité d'action collective. Depuis son entrée en vigueur, plusieurs associations ont adressé des plaintes collectives auprès de la CNIL. Par exemple, la Quadrature du Net a déposé une plainte aux noms de 12 000 personnes en mai 2018 contre Google, Apple, Facebook, Amazon et LinkedIn ; l'ONG Noyb *(None of Your Business)* sur les cookies et le transfert de données en 2019 et 2020 ; ou encore la Ligue des Droits de l'homme en juin 2020 dénonçant les difficultés d'exercice du droit d'accès des chauffeurs auprès d'Uber. Ces dépôts de plainte collective présentent la caractéristique d'être médiatisés par ces organismes. Elles sont accompagnées de communiqués et de conférences de presse et font l'objet de relais dans les médias. Autant que de changer une situation préjudiciable pour les individus, cette médiatisation vise à alerter l'opinion, provoquer un « scandale » et mettre ces problèmes à l'agenda du débat public.

Par ailleurs, la CNIL a également dans ses missions d'agir, sur demande ou d'initiative, contre des traitements réalisés ou envisagés, et souvent sur des comportements contestables exposés en public, en dehors du cadre spécifique du traitement des plaintes.

104 Vincent-Arnaud Chappe, *L'égalité au travail. Justice et mobilisations contre les discriminations*, Presses des Mines, 2019, 210 p.
105 Elles existent toutefois, à l'instar par exemple de la plainte récente déposée par la Ligue des droits de l'homme contre Uber afin que les chauffeurs puissent accéder aux données les concernant. https://www.liberation.fr/france/2020/06/12/la-ligue-des-droits-de-l-homme-depose-plainte-contre-uber-devant-la-cnil_1791034
106 À noter que certains plaignants publicisent toutefois leur plainte et leurs échanges avec les services de la CNIL sur les réseaux sociaux.

entre la personne qui demande ses données et l'entreprise concernée que la moindre friction va amplifier ce déséquilibre. C'est loin d'être anodin. Je place la responsabilité de ces obstacles en partie sur les entreprises, quoique certaines aient des raisons légitimes de faire preuve de prudence. Une série d'abus est possible[107]*. »* Cette absence de réponse conduit les individus à déposer plainte auprès de la CNIL espérant ainsi retrouver une prise sur l'organisme concerné. N'arrivant pas à résoudre la situation par eux-mêmes, l'appui de la CNIL doit faire évoluer le rapport de pouvoir en leur faveur.

Enfin, le cadre relationnel de certaines situations sociales asymétriques réduit les possibilités pour l'individu de faire entendre ses droits par crainte de répercussions. Ce dernier cas est fréquent dans les situations professionnelles : plusieurs plaignants mentionnent explicitement de préserver leur anonymat pour que leurs supérieurs hiérarchiques n'aient pas connaissance de leur dénonciation : *« pourriez-vous aussi garder mon identité anonyme par rapport à mon employeur »* (plainte, mai 2016), *« J'aimerais pouvoir rester anonyme »* (plainte, mai 2019). Ainsi, le rapport individuel au droit de protection des données personnelles est enserré dans des situations où les positions et ressources de pouvoir dans l'organisation varient. D'autres individus, disposant d'une position hiérarchique plus élevée, de ressources particulières ou encore du soutien d'un syndicat, sont insérés dans un champ de force qui leur est plus favorable et ne les contraint pas de recourir à la CNIL pour faire valoir leurs droits. D'autres à l'inverse, n'imaginent même pas contester une situation qu'ils jugent injuste et la subissent en silence.

Le plaignant perçoit la CNIL comme une ressource, qui lui permettra d'objectiver sa situation, de rationaliser son discours et de prendre appui sur le droit retrouver des « prises » face à une situation qui lui échappe et de faire évoluer le rapport de force en sa faveur.

> *Un petit peu dépités par l'imprenable forteresse YouTube qui se dresse devant nous, nous vous contactons afin de solliciter votre aide pour faire retirer cette fameuse vidéo.*
>
> **(Plainte, mai 2016)**

> *Veuillez trouver ci-joint une réclamation que j'ai envoyée à la société XXX, pouvez-vous m'apporter votre aide car je n'y arrive pas toute seule. J'ai réclamé par mail auprès de leurs services plusieurs fois sans résultats, je me retourne vers vous.*
>
> **(Lettre tapée, mai 2016)**

> *Devant leur obstination, je vous sollicite afin que vous fassiez pression sur leurs services pour effectuer ce défichage, dans les plus brefs délais.*
>
> **(Lettre tapée, mai 2016)**

Un nombre très important de plaintes et de courriers contient des expressions telles que *« Je ne sais plus quoi faire »*, *« Ras le bol »*, *« J'en ai marre »*, *« Je suis fatigué »*, etc. qui témoignent de la lassitude des individus, engagés dans des démarches longues et infructueuses, et ressentant une impuissance pour résoudre leur problème. Face à ces difficultés, on peut faire l'hypothèse que nombre d'individus n'ont pas recours à leurs droits. Plutôt que de s'engager dans un acte de dénonciation *(voice)*, ils acceptent ou subissent en silence la surveillance *(loyalty)* ou se tournent vers d'autres environnements et infrastructures techniques, voire n'ont plus recours au numérique *(exit)*[108]. Comme le déclare la sociologue Bénédicte Rey, *« le fait d'engager des démarches d'ordre réglementaires et juridiques nécessite donc pour l'usager d'investir des ressources temporelles et cognitives, ce qui représente un coût non négligeable pour un résultat incertain »*[109].

Ce coût nécessaire induit de fait des inégalités dans le recours aux droits entre les individus[110]. En effet, tous n'ont pas le temps, les connaissances, l'argent suffisant à consacrer à la protection de leurs données personnelles. Selon les dispositifs matériels d'accès aux droits mis en œuvre par les organismes et les compétences dont sont dotées les individus, les chemins du droit s'allongent et se complexifient pour certains. Dès lors, même si le nombre de plaintes reçues par la CNIL augmente chaque année, il est certain qu'encore trop peu de collectes et de traitements de données non conformes sont perçus et combattus par les individus.

---

107 Cité par Le Temps, https://labs.letemps.ch/interactive/2020/longread-donnees-personnelles/

108 Selon Albert Hirschman, les usagers ont le choix entre trois comportements face à la défaillance d'une institution publique ou privée : la défection (exit), la prise de parole (voice) ou le statu quo (loyalty). Albert Hirschmann, *Défection et prise de parole*, Fayard, 1970

109 Bénédicte Rey, *La vie privée à l'ère du numérique*, Lavoisier, 2012, p. 134

110 Les matériaux à notre disposition ne livrent que des fragments de description des situations sociales dans lesquelles sont placés les individus. Il conviendrait de compléter ces premières analyses par une enquête auprès de ces plaignants pour obtenir davantage d'informations sur les ressources, les contraintes et les rapports de pouvoir propres aux individus (leurs propriétés sociales) et aux groupes sociaux dans lesquels ils s'insèrent.

Au-delà des droits individuels, des leviers collectifs pour protéger la vie privée

« On comptait sur la nouvelle Intelligence
Artificielle pour résoudre les problèmes
de la planète.
Mais à chaque question,
elle répondait invariablement
qu'il lui manquait encore une donnée. »

François Houste, Mikrodystopies

Au-delà des droits individuels, des leviers collectifs pour protéger la vie privée

Les activités de la CNIL s'inscrivent, depuis 1978, dans le droit fondamental de chaque individu à la protection de ses données, de sa vie privée et de ses libertés devant le développement des systèmes informatisés. En étant ainsi dérivée de droits fondamentaux au cœur des démocraties modernes, la protection des données intègre un système normatif puissant et solidement ancré dans les sociétés occidentales. Ces droits individuels posent cependant la question du rapport au collectif et de la manière dont il serait possible de les faire respecter non plus dans une relation asymétrique, où l'individu, seul face à un organisme, cherche l'appui d'une autorité aux moyens nécessairement limités, mais dans des rapports de force plus équilibrés entre groupes sociaux. Aujourd'hui, la CNIL fait en sorte de répondre au mieux aux besoins du plaignant et, le cas échéant, enclenche des mesures depuis le contrôle jusqu'aux sanctions afin de mettre en conformité les acteurs qui n'auraient pas respecté le cadre (voir infographie page 42). Elle tire souvent, de situations individuelles, une analyse qui concerne un large groupe de personnes, utilisateurs ou employés de l'organisme mis en cause et les plaintes constituent pour elle un capteur fin des attentes de la société. Pourtant, elle reçoit plus de 14 000 demandes

Pexels cc-by Ann H

de plainte chaque année et ses moyens, s'ils augmentent, permettent difficilement de répondre dans un temps court à autant de questions et de sollicitations individuelles.

La mission de la CNIL s'inscrit avant tout dans le rôle de « gardienne des droits et des libertés » : le régulateur n'a pas vocation à être seulement le « gendarme des données personnelles », ou « les forces du RGPD ». Une meilleure compréhension des raisons pour lesquelles les personnes se retrouvent en situation de faire valoir leurs droits auprès de la CNIL et une connaissance plus fine des ressorts individuels et collectifs de la protection de leurs libertés par les individus doivent nous permettre de répondre à ces enjeux. Le levier de la CNIL reste la mise en conformité des acteurs (responsables de traitement), par le volet répressif, mais aussi par l'accompagnement et la production des outils qui leur permettront de mieux prendre en compte le RGPD et les différentes lois applicables.

La CNIL n'est pas seule face aux individus d'une part, aux responsables de traitements d'autre part. Les droits individuels sont aussi une affaire collective. Associés aux actions de la CNIL, la constitution de nouveaux corps intermédiaires de la donnée, la prise en compte de ces sujets par des syndicats, mais aussi les actions des associations, de l'État et des collectivités locales, les apports de la recherche, peuvent permettre de renforcer la protection des données et de la vie privée. Cette série de recommandations donne des pistes en ce sens.

POURSUIVRE LES TRAVAUX ENGAGÉS, EN INTERNE ET AVEC LES MILIEUX DE LA RECHERCHE

Ce cahier Innovation et prospective revient sur l'histoire de la protection de la vie privée, puis, dans une démarche compréhensive, sur les pratiques ordinaires en matière de gestion des données personnelles par les individus. Il inclut un exercice inédit d'analyse qualitative des plaintes reçues par la CNIL. Cette étude réalisée en interne invite à prolonger des travaux de recherches, en lien avec le milieu académique, pour mieux comprendre les usages numériques et les parcours du droit des individus. Cette connaissance est nécessaire à l'institution pour accompagner les individus dans la protection de leurs données et de leurs libertés.

Engager des études pour mieux appréhender les usages numériques quotidiens

L'analyse exploratoire menée dans ce cahier sur les plaintes a ouvert une série de pistes que le LINC entend poursuivre dans les prochains mois. Il s'agit en premier lieu d'acquérir une meilleure connaissance des personnes qui s'adressent à la CNIL afin de déterminer si des variables socioéconomiques jouent un rôle dans la mise en œuvre des droits de protection des données personnelles. Parallèlement, nous

souhaitons engager un travail d'enquête qualitative auprès de plaignants afin d'affiner nos conclusions provisoires sur les parcours du droit, pour mieux comprendre les obstacles rencontrés et mieux accompagner, au quotidien, les individus, citoyens et consommateurs. Nous souhaitons notamment consolider le cadre d'analyse à double entrée, mobilisant à la fois les étapes des recours aux droits telles que définies dans la partie 4 (rendre visible l'infrastructure, se considérer comme victime et un rapport asymétrique) et les motifs de sollicitation et de plainte identifiés dans la partie 3 (fichage administratif, prospection commerciale, enjeu réputationnel et surveillance au travail). Cela permettrait d'identifier plus clairement les leviers actionnables pour rendre ces recours moins sinueux pour l'individu.

Plus généralement, la CNIL doit renforcer son analyse des usages, pour mieux comprendre comment les gens se débrouillent avec le numérique et gèrent la circulation de leurs informations personnelles dans différents secteurs (éducation, travail, services publics, loisirs, etc.). Une compréhension située de ces usages et des logiques qui les guident est nécessaire pour adapter les politiques de prévention et l'accompagnement des individus dans leur diversité. Cette recommandation appelle au développement de travaux empiriques complémentaires sur les usages numériques et les pratiques quotidiennes en matière de protection des données personnelles.

Étendre nos collaborations avec la recherche

Dans cette optique, la CNIL, via le LINC approfondira ses relations avec les milieux de la recherche dans une logique interdisciplinaire. Les liens de la CNIL avec la recherche sont anciens, prenant la forme de partenariats (Inria, IMT), ou de collaborations au cas par cas avec des équipes de recherche sur des projets d'intérêt commun. Le LINC entend développer ses collaborations à partir de 2021, en abordant notamment les outils de mise en visibilité des infrastructures de collecte de données, la compréhension des usages numériques et les parcours du droit des individus.

RENDRE VISIBLES LES INFRASTRUCTURES DE DONNÉES

Produire de la régulation par des incitations réputationnelles *(sunshine regulation)*

Les effets réputationnels sont un levier important pour la mise en conformité des acteurs[111]. La crainte d'une réputation négative, ayant un effet sur la confiance des utilisateurs, et *in fine* sur leur modèle économique, peut conduire des entreprises à opter pour des pratiques exemplaires en matière de protection des données personnelles. Dès lors, parier sur la publicité et la mise en transparence des pratiques des acteurs afin que le grand public en tire ses propres conclusions aura pour conséquence possible de leur permettre de choisir de quitter un service aux mauvaises pratiques, ou bien d'inciter l'organisme à modifier ses comportements. Les mises en demeure et les sanctions publiques prononcées par la CNIL y contribuent également, au-delà des seuls organismes mis en cause par celles-ci. En parallèle, la CNIL développe au sein du LINC des outils de mise en visibilité des pratiques des acteurs du numériques, afin de donner à voir des infrastructures parfois inconnues des utilisateurs. Le LINC a lancé en septembre 2020 une nouvelle version de son logiciel CookieViz[112], un outil de visualisation pour mesurer l'impact des cookies et autres traceurs lors de la navigation en ligne, ainsi qu'une visualisation des interactions entre les différents acteurs de la publicité en ligne[113]. Un observatoire des cookies vient compléter la démarche, dont l'objectif est de mettre en visibilité les pratiques des acteurs de la publicité en ligne afin que chacun (grand public, société civile, médias) puisse avoir les outils pour suivre en temps réel l'évolution du secteur. D'autres projets sont envisagés, comme un projet de cartographie des fichiers de données personnelles détenus par le secteur public ou d'analyse des partages de données dans les objets connectés.

La CNIL avait déjà proposé ce type de régulation dès 2014 avec le projet Mobilitics (mettre en lumière la transmission des données des applications des smartphones et le rôle de l'identifiant publicitaire[114]) et, à propos des pratiques de design, en 2019, notamment pour mettre en lumière et débat les pratiques de design trompeurs ou abusifs *(dark patterns)*. On pourrait de la même manière imaginer des

111 Le rôle des incitations réputationnelles dans la régulation, Séminaire du Club des Régulateurs, Université Paris-Dauphine, 18 octobre 2019, https://chairgovreg.fondation-dauphine.fr/sites/chairgovreg.fondation-dauphine.fr/files/attachments/synthe%CC%80se_191018_0.pdf
112 https://linc.cnil.fr/fr/cookieviz-une-dataviz-en-temps-reel-du-tracking-de-votre-navigation
113 Voir par exemple : https://linc.cnil.fr/visualiser-le-web-publicitaire-avec-les-fichiers-adstxt-et-sellersjson
114 https://linc.cnil.fr/sites/default/files/typo/document/Lettre_IP_N-8-Mobilitics.pdf

moyens de rendre visibles les cas pour lesquels les personnes sollicitent la CNIL, la prospection commerciale, la surveillance au travail, certains fichiers de l'État, etc.

L'ensemble de ces actions aurait pour conséquence de faire sortir le sujet des seuls murs de la CNIL pour qu'il soit saisi par l'ensemble de la société, d'outiller les corps intermédiaires (voir infra), et d'appuyer les outils plus traditionnels dont dispose la CNIL.

Améliorer la visibilité des thématiques des plaintes individuelles reçues à la CNIL

La CNIL publie chaque année dans son rapport annuel, accessible à tous, les statistiques des plaintes reçues sur la période, avec des indications sur les secteurs et les cas qu'elle a eu à traiter. Pour accroître la visibilité de ces chiffres annuels, il pourrait être intéressant en parallèle de développer des outils de visualisation plus dynamique de ces plaintes, par exemple un tableau de bord accessible sur le site, ou une datavisualisation. Par ailleurs, des travaux pourraient être lancés pour intégrer la grille d'analyse produite dans les parties 3 et 4 de ce cahier.

Une telle mise en lumière et des rendez-vous réguliers pourraient ainsi transformer ces plaintes individuelles en problèmes qui doivent être débattus et traités à l'échelle collective. L'intégration de témoignages de plaintes anonymisées (tels qu'ils existent déjà dans les rapports annuels) bénéficierait en outre aux individus, pour faciliter la prise de conscience que leur situation individuelle est partagée par un grand nombre de personnes et peut être corrigée. Cela permettrait la constitution de groupements de victimes qui pourraient porter collectivement ces problèmes et inverser les rapports de force entre victimes et responsables. Il donnerait également à la société civile (corps intermédiaires et associations) et aux médias de la matière pour engager des leviers d'action.

Rendre visibles les failles des systèmes

La question de la visibilité des traitements de données, mais également celle des « failles », sont au cœur des évolutions de la protection des données proposées depuis 2018 par le RGPD. D'abord, les obligations d'information et de consentement ont été renforcées pour améliorer la prise de conscience des personnes concernées quant à l'utilisation de leurs données personnelles. De nouvelles dispositions ont été introduites comme l'obligation de notifier une violation de données aux personnes concernées en cas de risque élevé pour elles (art. 34 du RGPD) dont l'objectif affiché est de rendre visible des atteintes aux données pour que les personnes puissent prendre leurs dispositions. Par ailleurs, l'obligation nouvelle de tenir un « registre des traitements » a conduit de nombreux organismes, entreprises et administrations à mettre en place une réelle gouvernance des données pour mieux suivre les données utilisées et éviter les incohérences. Une première étape de visibilisation de ces failles a été franchie avec l'ouverture des données relatives aux notifications reçues par la CNIL afin de constituer des indicateurs ou des baromètres[115]. Des travaux sur les moyens permettant aux individus de connaître plus facilement si une de leurs données a été diffusée ou corrompue pourraient être engagés.

ENCOURAGER LE DÉVELOPPEMENT ET LA CRÉATION DES CORPS INTERMÉDIAIRES DE LA DONNÉE

Les situations menant les individus à contacter la CNIL, on le voit dans la partie 3 de ce cahier, reposent souvent sur une forme de détresse individuelle face à un événement ou à la répétition d'un événement du quotidien dont ils ne parviennent pas à se défaire.

Accompagner la prise en considération des données personnelles par les syndicats

Les plaintes liées à la surveillance au travail tiennent une place importante, notamment pour le recours à la vidéosurveillance. La pandémie du COVID-19, les différents confinements et la généralisation du recours au télétravail ont entraîné une recrudescence d'appels auprès de la CNIL pour des questions relatives au contrôle constant des salariés[116], le recours à la géolocalisation des véhicules des salariés se multiplie[117], de même que le contrôle d'accès biométrique sur les lieux de travail[118] – quelques exemples

115 Comme celui-ci : https://www.pwc.fr/fr/publications/data/barometre-data-breach.html
116 https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail
117 https://www.cnil.fr/fr/la-geolocalisation-des-vehicules-des-salaries
118 https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail

d'un champ dans lequel les « expérimentations » avec les droits et libertés des personnes sont très nombreuses.

La CNIL ne peut cependant porter seule ces questions et en direct avec les salariés. Si le cadre légal permet, avec des obligations d'information des personnes, et la garantie des droits du RGPD, de mettre en place un certain nombre de dispositifs, leur installation n'est cependant pas obligatoire, elle pourrait faire l'objet de négociations collectives avec les employeurs. Le numérique manque aujourd'hui de corps intermédiaires en mesure de prendre en charge les questions qui lui sont liées : il s'agirait d'en encourager une meilleure prise en compte par les syndicats traditionnels, mais aussi de voir naître de nouvelles formes de syndicats et instances représentatives des salariés et des travailleurs indépendants (voir encadré). Historiquement, il est intéressant de noter que les syndicats sont des interlocuteurs de la CNIL depuis sa création[119]. À titre d'exemple, en 1980, le Syndicat de la magistrature, la Confédération syndicale du cadre de vie, la CGT, la CGC, la CFDT et la Fédération des travailleurs du livre figuraient parmi les organisations syndicales qui avaient adressé des plaintes à la CNIL[120].

Zoom sur…

Des initiatives existent déjà : la CGT, la CFDT, FO, l'UNSA accompagnent déjà ou cherchent à accompagner les travailleurs des plateformes. Des nouvelles formes de représentation apparaissent au Royaume-Uni et en Europe autour de l'initiative de l'ONG *Worker Info Exchange*, qui entend par exemple aider les travailleurs du numérique à se réapproprier leurs droits sur les données collectées qui les concernent. Au Royaume-Uni, l'ADCU (*App Drivers and Couriers Union*) engageait en 2020 une action collective des chauffeurs Uber et Ola Cabs de demande de droits d'accès et portabilité des données afin de produire un « data trust », un commun de données destiné à faire valoir leurs droits auprès des plateformes (qui contrattaquaient en justice en décembre 2020).

La question de l'usage des données personnelles au travail pourrait faire l'objet de démarches et des négociations collectives, mais aussi permettre d'informer certains managers et responsables d'entreprises des droits de leurs salariés. Les syndicats et nouvelles formes d'organisations pourraient également se saisir de l'article 77 du RGPD, qui ouvre la possibilité pour l'introduction de plaintes collectives.

La CNIL pourrait accompagner ce mouvement par la production de boîtes à outils à destination des salariés, mais aussi à destination des employeurs qui, pour les plus petites entreprises, peuvent ne pas respecter le cadre par simple méconnaissance de celui-ci.

Renforcer les liens avec le monde associatif et notamment les associations de consommateurs et les associations de défense des libertés publiques

« La Commission a été saisie à plusieurs reprises de réclamations de personnes physiques se plaignant d'être importunées par une publicité leur parvenant à leur domicile sans qu'ils l'aient voulue, et quelquefois ce qui est manifestement plus grave, au lieu de leur travail. »

1978 – 1980, extrait du 1er Rapport annuel de la CNIL

La prospection commerciale figure encore en 2021 parmi les cas les plus nombreux de plaintes. Elles restent l'une des raisons historiques pour lesquels les personnes s'adressent à la CNIL (voir encadré). Plus largement, les individus dans leur statut de consommateur font face à la collecte et aux traitements de leurs données à grande échelle, par les entreprises avec qui elles ont des relations, au travers du dépôt de cookies à finalités publicitaires, etc.[121]

119 Il convient également de relever que le collège de la CNIL comprend, parmi ses membres, deux représentants du CESE dont l'un est souvent issu d'un syndicat.
120 https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_1er_rapport_dactivite_1978-1980_vd.pdf
121 La CNIL consacre une large partie de ses activités à ce type de traitement et à la régulation de ces secteurs, comme en témoignent par exemple la recommandation cookies et autres traceurs publiée en septembre 2020, ou les sanctions données à Google et Amazon en décembre 2020.

Les actions menées par les associations de consommateurs sur la base de la collecte et du traitement des données personnelles correspondent à un mode différent et complémentaire, un levier d'action à encourager pour enjoindre les sociétés concernées à respecter le cadre légal, voire à demander des réparations[122]. La CNIL collabore notamment avec l'UFC Que Choisir pour intégrer la notion de protection des données personnelles dans l'analyse des produits effectuée par celle-ci, et publiée dans son magazine.

Les liens sont nombreux entre la protection des données et la protection des consommateurs, comme en témoigne le protocole de coopération entre la CNIL et la DGCCRF, signé dès 2011 et actualisé en 2019, visant notamment à « mieux sensibiliser les consommateurs et réaliser des contrôles communs ». Ces liens, avec le régulateur et avec les associations de consommateurs sont à renforcer afin de répondre au mieux aux besoins des personnes.

Par ailleurs, le tissu des associations de défense des libertés et des droits de l'homme – notamment de libertés numériques réunies au sein du réseau European Digital Rights (EDRi) et plus largement celles représentées au sein de la Commission Nationale Consultative sur les Droits de l'Homme (CNCDH) – joue un rôle crucial pour rendre visible les dispositifs de collecte et de traitement de données personnelles, sensibiliser l'opinion et faire émerger des problèmes publics devant être pris en charge par les pouvoirs publics.

De la création des autorités de régulation dans les années soixante-dix jusqu'à de récentes décisions de la Cour de Justice de l'Union européenne, les mobilisations de la société civile sont centrales dans l'évolution de la régulation en matière de données personnelles, et contribue à la prise en compte de ces questions dans les débats publics, et par le législateur.

Ces associations peuvent agir, comme elles en ont déjà eu l'occasion par le recours à l'article 77 du RGPD et aux plaintes collectives auprès de la CNIL. Elles ont également leur rôle à jouer – avec la CNIL, et dans un rôle différent –, pour faire évoluer les mentalités dans la société civile, les organisations publiques et privées, ainsi que le champ politique.

Encourager les initiatives de production collective et open source de nouveaux standards techniques

Face à l'uniformisation des outils et services numériques proposés par les grandes plateformes selon des standards majoritairement étatsuniens, les individus soucieux de la protection de leurs données peuvent avoir recours à des « tactiques » de contournement, parfois rudimentaires (page 17). S'il est nécessaire d'outiller les individus afin qu'ils puissent numériser et automatiser ces contournements, la proposition de services alternatifs et le développement des communautés de développeurs et de porteurs de projets et solutions vertueuses du point de vue de la protection des données est à encourager et à accompagner.

À titre d'exemple, de telles initiatives sont en cours dans le domaine de la portabilité des données, afin de produire des standards communs, portées par des associations et des collectifs d'entrepreneurs, repris en partie à l'échelon européen dans le *Data Governance Act*, en cours de négociation à la Commission européenne. Le LINC propose déjà une cartographie des outils et pratiques de protection de la vie privée (voir plus bas), mais chaque secteur et chaque type de service pourrait de la même manière œuvrer à la création de standards communs, différents des standards de fait imposés par les plus grandes plateformes (cette proposition figurait déjà pour les pratiques de design dans notre cahier IP6, page 42)[123]. Il est également important d'inciter et encourager les briques techniques qui jouent aujourd'hui le rôle de porte d'accès à des contenus ou des services – navigateurs, systèmes d'exploitation mobiles, réseaux sociaux – offrent des interfaces et des environnements de développement ouverts pour permettre à des tiers de proposer des outils, logiciels et extensions qui renforcent la protection des données.

L'enjeu pour les solutions et les standards protecteurs de la vie privée reste le passage à l'échelle afin de bénéficier des effets réseaux qui leur permettront de se développer. L'exemple de la messagerie Signal et de l'explosion de son nombre d'utilisateurs à l'occasion de la modification des conditions d'utilisation de Whatsapp en février 2021 démontre que les utilisateurs sont prêts à tester et migrer vers de nouveaux services.

122 L'association UFC Que Choisir avait obtenu la condamnation de Twitter par le TGI de Paris, le 7 août 2018 et, à supprimer plus de 250 clauses abusives et/ou illicites présentes dans ses conditions d'utilisation et sa politique de confidentialité. Dans un jugement du TGI de Paris du 12 février 2019, le retrait par Google de 209 clauses abusives et illicites, donc certaines « règles de confidentialité ». La CNIL avait répondu à l'alerte donnée par l'association en décembre 2016 à propos d'un défaut de sécurisation de certains jouets connectés, qui avait donné lieu à la mise en demeure publique du fabricant de la poupée Cayla.
123 https://www.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip6.pdf

PRODUIRE DE LA PRÉVENTION POSITIVE DES USAGES DU NUMÉRIQUE ET DE LA PROTECTION DES DONNÉES PERSONNELLES

Ne pas considérer la victime comme (ir)responsable

Considérer les victimes comme responsables revient à les considérer irresponsables. La protection de la vie privée et des données, si elle touche à l'intime, n'en reste pas moins une question qui doit être débattue à l'échelle collective, de l'organisation de la collecte et du traitement de données (systèmes dans lequel sont pris les individus). Comme nous le développons dans la partie 2, page 20, les individus sont confrontés « à de multiples microdécisions qu'ils ont à prendre sans que le risque pour leur vie privée soit toujours priorisé », mises en tension avec « d'autres impératifs et intérêts en jeu dans les différentes sphères de leur existence, comme la vie professionnelle, amicale, familiale ou publique ». Chacun est amené à faire des choix dans l'usage des outils du numérique, avec la volonté de ne pas se couper de ses liens sociaux, notamment chez les plus jeunes et les adolescents. Ni vraiment victime, ni irresponsable, chacun fait ses choix en fonction des paramètres qu'il ou elle a à prendre en compte. La prévention ne doit pas avoir pour objet la mise au ban de certaines pratiques numériques ou l'usage de certains services.

À ce titre, les politiques de prévention ne peuvent avoir pour objet de rendre responsables les personnes des préjudices qu'elles pourraient avoir à subir du fait du traitement de leurs données personnelles, ou de la visibilité de leur image et leur profil, par exemple. Comme nous l'analysons dans la partie 2, la responsabilisation des individus produit des effets pervers : en se sentant coupables de leurs comportements, les victimes n'attribuent pas la responsabilité de leur situation à un tiers et la subissent plutôt que de s'engager dans un processus de mise en œuvre de leurs droits. Il y a ainsi un risque à se focaliser sur l'individu et ses pratiques plutôt que de mettre en cause les institutions et les structures qui placent les individus en situation problématique.

Protéger le contexte

L'importance que la CNIL donne à la protection des données ne doit pas conduire à viser l'objectif que chaque individu est pleinement conscient, à tout instant et dans toutes situations, de ses droits et des choix qu'il a la possibilité de faire. Si la protection des données est souvent un paramètre mineur dans une décision individuelle, c'est bien souvent parce que les individus souhaitent bénéficier d'une protection « automatique », qui ne dépendrait pas de leur capacité à consentir ou à s'opposer. La notion d'« intégrité contextuelle » développée dans ce cahier doit être considérée de manière plus systématique par les organismes pour limiter les traitements de données à des opérations qui sont « raisonnablement attendues » par les personnes concernées et éviter, au maximum, des utilisations éloignées du contexte dans lequel la personne est placée.

Une vigilance particulière doit ainsi être portée aux pratiques mises en place par les acteurs majeurs du numérique depuis une vingtaine d'années pour « normaliser » des pratiques décontextualisées comme le célèbre « nous traitons vos données pour l'amélioration de nos services », dont l'imprécision contribue à minorer l'importance du contexte. En la matière, il semble pertinent de se référer à la notion d'honnêteté commune (« *common decency* ») proposée par George Orwell pour caractériser le fonctionnement d'une société démocratique pour encourager des approches qui ne consistent pas à traiter massivement, de manière indifférenciée et sans raison réelle des données sur les personnes.

Adapter les politiques et campagnes de prévention

Les discours éducatifs sur le numérique sont indispensables pour fournir connaissances et ressources aux individus, qu'ils soient particuliers ou professionnels. Aujourd'hui concentrés majoritairement vers les jeunes et les publics éloignés du numérique, il faudrait en premier lieu renforcer les possibilités d'apprentissage tout au long de la vie, puisque les besoins en compétences évoluent. En outre, pour rencontrer l'adhésion, ces messages et campagnes doivent être adaptés selon les individus et ancrés dans leurs pratiques numériques par des exercices et conseils concrets (cela nécessite ainsi préalablement de renforcer notre connaissance des usages numériques par le biais d'enquêtes).

Comme le déplore Anne Cordier : « *Dire par exemple à un enfant de 8 ans qu'il faut faire attention aux informations qu'il laisse en ligne parce que son futur employeur pourra tomber dessus, ça ne fait aucun sens pour lui, il est bien trop*

éloigné du monde du travail ! »[124]. Pour y remédier, il faut partir de situations quotidiennes, investir différents médias et pluraliser les messages selon les cibles. Enfin, plutôt que de culpabiliser les individus en pointant les mauvaises pratiques, les politiques de prévention gagnerait à fournir des clés de compréhension sur le fonctionnement des technologies numériques et de leur écosystème.

Faire de l'inclusion et de l'éducation à la protection des données des priorités publiques

L'inclusion et l'éducation sont des dimensions des politiques numériques en France qui se sont avérées insuffisantes, comme l'illustre l'histoire des « plans » de numérisation depuis les années 60. À l'échelle locale ou nationale, les politiques orientées vers l'attractivité, l'innovation et le développement économique ont plus souvent rencontré l'intérêt des décideurs que celles sur les pratiques quotidiennes des individus. Les individus sont implicitement considérés comme autonomes pour acquérir les connaissances et compétences nécessaires à l'inclusion dans notre société numérique. Les inégalités face au numérique s'intensifient comme la crise sanitaire du Covid-19 l'a mis en lumière.

Si les nouvelles approches en la matière reposent d'abord sur une multitude d'acteurs publics, privés et associatifs, ceux-ci mettent en place des solutions partielles, s'adressant à certains publics, de façons très disparates selon les territoires et promouvant des messages variés, sans que l'on sache précisément qui pilote cette politique et quelles sont ses finalités et sans que des financements réguliers et nationaux servent à consolider cet écosystème. Il est souvent difficile pour les individus de se repérer dans un paysage mouvant de structures et de programmes d'accompagnement.

Pour y remédier, le secrétariat d'État au numérique a lancé en septembre 2020 un plan de relance en faveur de l'inclusion numérique, avec pour objectif de « *porter un coup d'accélérateur inédit à l'inclusion numérique* ». Ce plan vient renforcer le Plan national pour un numérique inclusif (septembre 2018) et vise notamment à « *outiller les aidants numériques qui accompagnent les Français qui ne seront jamais autonomes vis-à-vis du numérique* », par la « *généralisation du service public numérique Aidants Connect et la montée en compétence numérique des aidants professionnels* », et « *proposer des formations pour les particuliers* », au travers de 4 000 conseillers numériques. La conception et le déploiement de kits d'inclusion numérique accessibles et attractifs à destination des structures de proximité figure également au projet.

La thématique de la protection des données et de la vie privée doit figurer dans ce plan d'inclusion au numérique. On l'a vu (page 24), si les sujets portés par la CNIL ne sont pas toujours prioritaires pour les personnes les plus éloignées du numérique, elles peuvent néanmoins ressentir des troubles dans leur quotidien et notamment dans l'accès à certains services. Les personnes éloignées, ou peu pratiquantes du numérique doivent acquérir les bases afin de comprendre leurs droits, et comment les faire-valoir. En 2019, la CNIL a publié un kit d'information à destination des travailleurs sociaux pour protéger les données de leurs publics[125]. Dans cette continuité, la CNIL pourrait travailler sur la définition de recommandations fondées sur les besoins réels que les échanges avec les acteurs de l'inclusion numérique pourraient faire remonter.

La dématérialisation de l'État et la multiplication de nouveaux services numériques obligent certaines personnes non-utilisatrices du numérique à s'y confronter, et avec eux, les accompagnants et aidants. Cette transition pousse notamment certains médiateurs numériques dans une position d'accompagnateur social plus que numérique. Il semble donc nécessaire de penser à la formation d'un rôle d'accompagnement mixte, qui permettrait de conjuguer l'accès à des prestations sociales à des compétences numériques.

Enfin, on se focalise souvent – et à juste titre – sur les populations les plus éloignées du numérique, les personnes n'ayant pas les compétences numériques de base. Or, il existe une multitude de processus d'exclusion par le numérique, plus ou moins importants, inscrits dans les routines quotidiennes. Des personnes a priori éloignées ou en difficulté peuvent avoir des pratiques numériques riches. Un individu peut être autonome pour certaines démarches mais pas du tout pour d'autres. Les compétences numériques ne se valent pas en soi : elles dépendent des situations d'usage spécifique. Dans les usages routiniers, se nichent des peurs et des appréhensions relatives notamment à la maîtrise de ses données personnelles. Par exemple, le paiement en ligne est un acte qui fait peur à un grand nombre de personne. Dès lors, il vaudrait mieux se focaliser sur les situations plutôt que les profils, les épreuves rencontrées par les individus plutôt que les catégories.

124 https://linc.cnil.fr/anne-cordier-la-socialisation-un-effet-majeur-sur-les-pratiques-des-jeunes-en-matiere-de-protection
125 https://www.cnil.fr/fr/travailleurs-sociaux-un-kit-dinformation-pour-proteger-les-donnees-de-vos-publics

Travailler sur les imaginaires: rendre désirable la protection des données

Pour accompagner la prévention, développer une culture du risque et rendre désirable la protection des données, il est nécessaire de cultiver de nouveaux imaginaires. Les sociétés se construisent par les mythes et la poésie comme l'ont analysé les anthropologues. Imaginer, créer et raconter des histoires autour de la place des technologies numériques dans nos sociétés, et en particulier des données personnelles, permet de se projeter dans le futur, tant à l'échelle individuelle que collective, d'en débattre et de mettre en place les conditions pour le faire advenir – ou non.

Poser un regard différent sur le monde est porteur de perspectives et d'alternatives. Les imaginaires nous permettent de repenser notre rapport aux données personnelles et de rendre perceptible ce qui est de l'ordre de l'invisible. C'est dans cette optique, que le LINC a organisé une collecte de fragments d'imaginaires et mis en place des ateliers internes de créativité. Nous recommandons de poursuivre et de multiplier ces expériences afin de constituer une bibliothèque collaborative des imaginaires relatifs à la protection des données personnelles. Parallèlement, la CNIL peut jouer un rôle pour stimuler la création artistique sur ces thématiques, par exemple en organisant des appels ou des concours (de nouvelles, de photos, etc.).

Fournir les outils pour l'autonomisation des acteurs

La loi pour une République Numérique affirme la mission de la CNIL de *« promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données »*. Sans se confondre avec les missions de certification ou de labellisation, prévues notamment par l'article 42 du Règlement général à la protection des données, la CNIL encourage et donne à voir différentes possibilités offertes pour que chaque individu soit en mesure d'adopter des outils « privacy friendly » dans ses usages du quotidien.

Dès 2017, un outil était lancé afin de permettre de rendre concret le droit au déréférencement en permettant également aux particuliers l'avancement et l'effectivité d'une demande[126]. La même année, le LINC a publié une cartographie des outils et pratiques de protection de la vie privée, recensant des « outils, services, objets ou astuces que les individus peuvent utiliser dans leur vie quotidienne avec pour but explicite ou implicite de protéger leur vie privée »[127] . Cette cartographie pourra être mise à jour régulièrement et faire l'objet d'une communication plus importante auprès des individus.

De la même manière, la CNIL pourra, comme elle l'a déjà fait, valoriser des initiatives de bloqueurs de traceurs (cookies) dont le modèle économique reste vertueux, ou tout autre moyen permettant aux personnes de se protéger. Plus généralement, alors que les concepteurs de services numériques sont toujours à la recherche d'une plus grande fluidité, l'analyse menée dans ce cahier démontre à l'inverse que les moments de choix ou de paramétrages sont particulièrement importants pour se rendre compte des données collectées. Dès lors, comme nous l'avons déjà recommandé dans nos précédentes publications[128], nous préconisons d'entretenir des « frictions désirables », qui appellent l'attention des utilisateurs sur les traitements de données.

Ces outils ne viennent pas se substituer à l'obligation pour les responsables de traitement de se conformer aux règles de protection des données, mais ils viennent en complément, pour offrir les moyens aux personnes de leur autodétermination informationnelle.

126 https://linc.cnil.fr/fr/outil-controlez-votre-dereferencement
127 https://linc.cnil.fr/fr/une-cartographie-des-outils-et-pratiques-de-protection-de-la-vie-privee
128 Cahier IP 6, *La forme des choix* ; Livre blanc, *À votre écoute*

Zoom sur…

Pour une prise en compte globale des enjeux du numérique par les services publics

La réception par la CNIL de nombreuses sollicitations ne relevant pas de ses compétences et pointant vers des enjeux plus globaux de l'utilisation du web et des différents services et outils numériques met en exergue les difficultés d'orientation et d'information du public lorsqu'il fait face à une situation problématique. Les impacts que peut avoir cette absence ne sont pas anecdotiques pour les individus (atteinte psychologique, morale, financière, etc. – voir la partie 3).

Dans bien des cas, la CNIL redirige et guide les individus vers d'autres voies de recours, d'autres institutions, qui sont les compétents ou référents sur des problématiques précises, mais illisibles voire invisibles pour les personnes. Il semble alors nécessaire de pouvoir clarifier ces parcours pour les individus afin que ceux-ci puissent, dès la confrontation à une situation problématique, savoir à qui ils doivent s'adresser pour résoudre leur cas. Mais, au-delà de la méconnaissance des recours déjà existants, les individus peuvent également connaître des situations dans lesquelles ils se retrouvent désemparés par une réponse négative ou l'absence de réponse d'un canal pourtant identifié comme correspondant à la résolution de leur problème (voir encadré *page 46)*. La CNIL se retrouve alors dans la situation de devoir aider la préparation de certains individus dans leur démarche de recours, notamment en aidant à qualifier la nature réelle du problème pour les orienter correctement.

Ce double enjeu – s'il est important pour la CNIL dans le sens où elle permettrait aux individus de faire plus facilement usage de leurs droits et à ses agents de consacrer plus de temps à des missions qui relèvent de leurs compétences – dépasse l'institution. Il y a une nécessité plus générale pour le gouvernement de trouver des solutions dans l'accompagnement de ces problèmes qui trouvent leurs racines à plusieurs échelles et dans des situations diverses. Et plus encore lorsque s'accélère la transformation numérique des services publics et leur dématérialisation.

Bien entendu, « résoudre Internet » est complexe, cela nécessite plusieurs types d'ajustements et des choix politiques mais il semble important de souligner les problématiques récurrentes des individus qui lui arrivent. Ainsi, il paraît important de considérer plus sérieusement les plaintes relatives au numérique, qui, comme nous l'avons vu tout au long de ce cahier, ne relèvent pas de situations anodines. Les recours entre particuliers concernant de la vidéosurveillance privée (par exemple, ayant trait aux relations de voisinage) ou encore, la question du harcèlement en ligne, représentent également une part non négligeable de sollicitations de l'institution. Il s'agirait de renforcer la formation des fonctionnaires (notamment de police et de gendarmerie) et leur donner les moyens d'enquête sur les contenus et comportements illicites en ligne, etc.

Le Comité de la **prospective**

La CNIL anime un comité de vingt-et-un experts aux profils et horizons variés, pour enrichir les réflexions prospectives et contribuer aux débats sur l'éthique du numérique. Être plus à l'écoute et plus ouverte sur l'extérieur, travailler en partenariat avec le monde de la recherche et de l'innovation, tels sont les objectifs poursuivis par la CNIL avec ce Comité.

Placé sous la présidence de la Présidente de la CNIL, **Marie-Laure Denis**, le comité est composé des personnalités suivantes :

EXPERTS EXTÉRIEURS

Pierre Bellanger,
pionnier des radios libres,
entrepreneur et expert de l'Internet.

Pierre-Jean Benghozi,
directeur de recherche au Centre National de la Recherche scientifique (CNRS), professeur à l'école polytechnique et professeur à l'Université de Genève.

Stefana Broadbent,
psychologue, anthropologue, professeure associée au département de design de l'école polytechnique de Milan.

Isabelle Bordry,
entrepreneuse, pionnière de l'industrie française des médias numériques.

Dominique Cardon,
sociologue, directeur scientifique du Médialab de Sciences Po Paris, membre du comité de rédaction de la revue Réseaux.

Milad Doueihi,
philosophe, historien des religions et titulaire de la chaire d'humanisme numérique à l'Université de Paris-Sorbonne (Paris IV), co-titulaire de la chaire du Collège des Bernardins sur l'humain au défi du numérique.

Célia Hodent,
psychologue spécialiste de l'application de l'expérience utilisateur dans la conception de jeux vidéo.

Claude Kirchner,
directeur de recherche Inria, directeur du Comité national pilote d'éthique du numérique (CNPEN), conseiller du Président d'Inria.

David Le Breton,
professeur de sociologie et anthropologie à l'université de Strasbourg.

Titiou Lecoq,
journaliste indépendante, blogueuse, essayiste et romancière, spécialiste de la culture web.

Philippe Lemoine,
entrepreneur et essayiste, Président du Forum Action-Modernités, président de la Fing.

Lionel Maurel,
directeur-adjoint scientifique à l'Institut national des Sciences Humaines et Sociales du CNRS - InSHS Institut des Sciences Humaines et Sociales, auteur du blog S.I.Lex, sur les transformations du droit à l'heure du numérique.

Cécile Méadel,
sociologue, professeure de l'Université Panthéon-Assas, responsable du master Communication et multimédia. Chercheuse au CARISM, chercheuse associée au Centre de sociologie de l'innovation (Mines-CNRS).

Tristan Nitot,
entrepreneur, auteur et conférencier sur le thème des libertés numériques, a fondé et présidé Mozilla Europe.

Éric Pérès,
secrétaire général de FO-Cadres, membre du Conseil économique, social et environnemental (CESE).

Antoinette Rouvroy,
juriste, chercheuse FNRS au Centre de Recherche Information, Droit et Société (CRIDS) de Namur.

Henri Verdier,
Ambassadeur pour le numérique.

Nicolas Vanbremeersch,
entrepreneur, président et fondateur de l'agence Spintank et du lieu de coworking Le tank.

Célia Zolynski,
Professeure agrégée de droit privé à l'École de droit de la Sorbonne - Université Paris 1 Panthéon-Sorbonne - Personnalité qualifiée au sein de la CNCDH et du CSPLA, Membre du Comité national pilote d'éthique du numérique.

MEMBRES DE LA CNIL

Bertrand Du Marais,
Conseiller d'État.

Valérie Peugeot,
chercheuse au sein du laboratoire de sciences sociales et humaines d'Orange Labs.

Collection Cahiers Innovation et Prospective

Au sein de la Direction des technologies et de l'innovation de la CNIL, l'équipe innovation, études et prospective pilote des projets d'études et d'explorations de sujets émergents liés aux données personnelles et à la vie privée. Ses travaux se situent à la rencontre entre innovation, technologies, usages, société, régulation et éthique.

La collection des cahiers IP, pour Innovation & Prospective, a vocation à présenter et à partager les travaux et études prospectives conduits par la CNIL. Il s'agit ainsi de contribuer à une réflexion pluridisciplinaire et ouverte dans le champ Informatique & Libertés et de nourrir les débats sur les sujets d'éthique du numérique.

Ce numéro est le 8ème de cette collection :

CAHIER IP 1 - Vie privée à l'horizon 2020
Paroles d'experts

CAHIER IP 2 - Le corps, nouvel objet connecté
Du Quantified Self à la M-Santé : les nouveaux territoires de la mise en données du monde

CAHIER IP 3 - Les données, muses et frontières de la création
Lire, écouter, regarder et jouer à l'heure de la personnalisation

CAHIER IP 4 - éd. Comité de la prospective : Partage !
Motivations et contreparties au partage de soi dans la société numérique

CAHIER IP 5 - La plateforme d'une ville
Les données personnelles au cœur de la fabrique de la smart city

CAHIER IP 6 - La forme des choix
Données personnelles, design et frictions désirables

CAHIER IP 7 - Civic Tech, données et *Demos*
Enjeux de données personnelles et libertés dans les relations entre démocratie, technologie et participation citoyenne

Retrouvez-nous aussi sur l'espace éditorial LINC (http://linc.cnil.fr).

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Avril 2021
Commission Nationale de l'Informatique et des Libertés
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07
Tél. +33 (0)1 53 73 22 22
ip@cnil.fr

www.cnil.fr

linc.cnil.fr

LINC
CNIL.