Christine Petr et Olivier Segard

Introduction
LES DONNÉES PERSONNELLES EN SOUS-MARIN DE NOS JOURNÉES DIGITALES

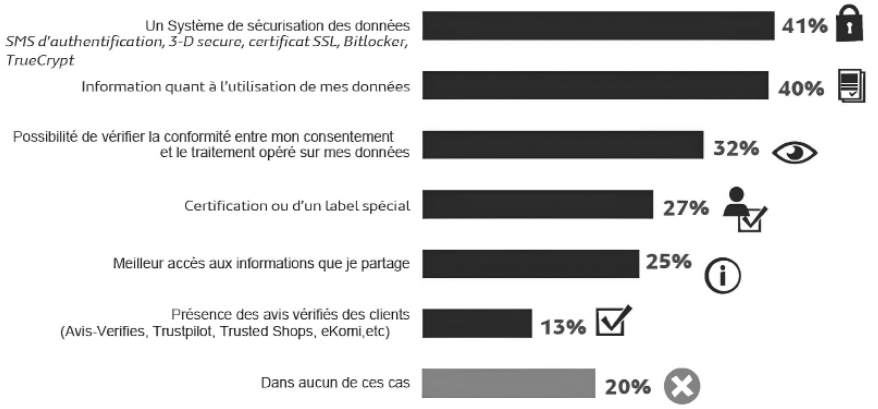
Contexte de l'ouvrage

Les promesses technologiques du numérique font l'objet de débats de société et d'échanges sur les enjeux techniques, économiques et éthiques spécifiques à la protection et au traitement des données personnelles. Soutenue partout en Europe par les organismes nationaux de régulation du numérique, telle la Commission nationale de l'informatique et des libertés (CNIL) en France, la question des données personnelles est renouvelée avec l'entrée en vigueur du Règlement général sur la protection des données (RGPD le 25 mai 2018), mais aussi avec la crise de confiance sur les réseaux sociaux numériques (par exemple le scandale Facebook-Cambridge analytica), l'arrivée massive des objets connectés, et les possibilités accrues d'exploitation des données *via* le *big data* et l'intelligence artificielle. Même si une étude parue en 2019 montre que 28 % des personnes interrogées pensent que la protection de leurs données personnelles sur Internet s'est améliorée depuis l'instauration du RGPD (Waelbroeck *et al.*, 2019), toujours selon la même étude il existe une demande pour plus de garanties et de réassurance comme le montre la figure page suivante (*ibid.*, p. 53).

La question des données personnelles et de leur gestion a toujours été l'objet de tensions entre le dévoilement nécessaire pour obtenir des bénéfices comme des offres de réduction, des cadeaux, des services gratuits, partager des informations professionnelles, etc., et le souhait de préserver sa vie privée et le secret professionnel (par exemple ne pas dévoiler son algorithme ou sa base de données clientèle pour un entrepreneur). Ce qui est plus nouveau, c'est d'une part l'accroissement du nombre de données disponibles à la suite de l'utilisation croissante des outils numériques connectés. C'est d'autre part, l'inflation de la valeur monétisable de ces données qui sont dès lors au cœur des modèles d'affaires des *pure players*. Pour preuve, la valeur des données personnelles exploitées par un *pure player* peut être estimée par la valorisation boursière

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

de l'entreprise puisque l'intégralité de l'actif réside dans ces données (Mattatia, 2021). Toujours selon l'auteur, à titre d'exemple, considérant un *pure player* comme Facebook, cette valorisation était en avril 2021 d'environ 720 milliards de dollars pour 2,8 milliards d'utilisateurs ; ceci représente une valeur moyenne de 250 dollars par personne. Comment dans ces conditions ne pas céder à la tentation de capturer ces données personnelles ? Ne sont-elles pas aujourd'hui communément considérées comme l'or noir du XXIe siècle ?



Les internautes attendent plus de garanties et de réassurance (Waelbroeck et al.*, 2019, p. 53).*

Les tensions entre le dévoilement et la protection des données personnelles se retrouvent à différents niveaux chez toutes les parties prenantes avec toutefois des variations d'intensité selon que l'on soit en situation normale ou face à une crise. Ces tensions sont expérimentées dans le cadre de nos différents statuts (*i. e.* consommateurs, clients, usagers, habitants et résidents, membres d'association, citoyens, employés, parents, etc.) puisque nous sommes toujours et dans chacun de ces contextes, des producteurs et des pourvoyeurs de données.

Au-delà du cadre individuel, ces tensions existent aussi dans les entreprises et les institutions. Ainsi, les tensions entre dévoilement et protection concernent aussi les acteurs organisationnels qu'ils soient du monde public (secteur public, service de l'éducation, gouvernement, associations humanitaires, caritatives, fédérations de médecins, organismes de santé, structures supranationales, etc.) ou du monde privé (créateurs et producteurs de biens et services de consommation, opérateurs de services numériques, etc.). Enfin, ces tensions sont d'autant plus accrues que de nouvelles pratiques professionnelles se sont généralisées. Notons à ce titre le Bring Your Own Device (BYDO), qui consiste à utiliser son équipement informatique plutôt que celui de l'entreprise, et le télétravail. Ces nouveaux modes de travail qui ont été fortement développés avec la crise sanitaire, augmentent la porosité entre les mondes personnels et professionnels (Pellegrini, 2018). Créant un risque toujours plus grand de sécurité, ces

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

nouvelles pratiques complexifient encore la gestion de l'arbitrage dévoilement/protection que l'on considère la position de l'individu ou celle de l'organisation.

Une façon de remédier à ces problèmes serait-elle l'adoption d'une bonne « hygiène numérique » ? Cette expression qui est de plus en plus utilisée dans la société a un caractère impérieux. L'hygiène est en effet définie de la façon suivante : « l'ensemble des principes, des pratiques individuelles ou collectives visant à la conservation de la santé, au fonctionnement normal de l'organisme » (Dictionnaire Larousse). Par extension, nous proposons de définir l'hygiène numérique individuelle comme « l'ensemble des principes et pratiques numériques, adoptés par les individus, dans leurs cadres personnels et organisationnels, impliquant des mesures de contrôle et de protection des données personnelles et visant un usage raisonné des outils numériques ».

L'État essaie de favoriser une hygiène numérique si on s'en tient à l'initiative des « conseillers numériques France services » (ANCT, 2021). L'État a annoncé en 2021 le lancement du recrutement de 4000 de ces conseillers sur tout le territoire pour un budget de 250 millions d'euros : « Ils y proposeront des ateliers thématiques, des accompagnements personnalisés ou des aides ponctuelles aux usagers désireux d'améliorer leurs compétences numériques. Parmi ces ateliers, ils accompagneront les Français désirant apprendre à allumer, mettre à jour et utiliser un ordinateur, une tablette ou un téléphone portable, rechercher des informations et des contenus sur Internet, écrire, envoyer et recevoir des courriels (employeur, proches, administration), ou encore communiquer en vidéoconférence » (ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 2021). Avec cette initiative, l'État chercherait également à favoriser un usage citoyen mais aussi critique du numérique, dont en ce qui concerne la protection des données personnelles.

Comme cela a déjà été démontré, adopter cette stratégie individuelle d'une « bonne » hygiène numérique offre des avantages non négligeables dans l'usage quotidien de la multiplication des outils du monde digital que nous utilisons tous les jours pour travailler, surfer sur la Toile et communiquer. Entre autres, en nous permettant de protéger et d'assurer une sécurité relative des données personnelles, ces réflexes et « bons » gestes permettent *in fine* d'allonger la durée de vie des outils (Raimondo, 2021).

Objet de l'ouvrage

L'objet de cet ouvrage est de présenter les défis et enjeux de la protection de la vie privée, qui fait désormais face à une collecte de données systématisée et à leur publication souvent volontaire sur les espaces numériques. En proposant une pluralité d'angles de vues disciplinaires (droit, sociologie, économie, psychologie, sciences politiques, sciences de gestion, philosophie, sciences du langage et de la cognition, etc.), l'ambition de cet ouvrage est de souligner que le

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

sujet de la protection de la vie privée n'est pas uniquement individuel, mais qu'il implique les collectifs auxquels les individus appartiennent, qu'il s'agisse des organisations ou de la société civile, dans le cadre de l'intérêt national des pays.

Les contributions des auteurs répondent alors à l'intention de vulgariser l'état des connaissances et leurs conclusions sur les raisons de conserver un certain contrôle sur ce qui est dévoilé de la vie privée de chaque citoyen, usager et consommateur. Après avoir lu cet ouvrage, le lecteur aura pris conscience des effets délétères d'un laisser-faire sur la protection des données à caractère personnel, et il aura une meilleure compréhension du besoin de vigilance sur ce qu'il diffuse auprès des espaces numériques. En complément, il sera sensibilisé au besoin de réfléchir pour orienter ses pratiques, qu'elles soient privées, publiques ou politiques, vers une meilleure hygiène numérique.

Projet de recherche Sensibdata

L'ouvrage s'appuie sur les contributions et les travaux rassemblés à la suite du projet de recherche Sensibdata qui a été soutenu et labellisé par la Maison des sciences de l'homme en Bretagne en 2018. L'équipe de recherche pluridisciplinaire Sensibdata a été créée sur la thématique de la protection de la vie privée et du contrôle de la diffusion des données à caractère personnel face au constat suivant. Les individus déclarent généralement que le sujet des données personnelles est un sujet qui les préoccupe et ils annoncent majoritairement des intentions de protection de leurs données qui sont élevées. Cependant, dans les faits, leurs comportements d'usage des outils du numérique paraissent très laxistes, ou du moins désinvoltes quant à la maîtrise et à l'opposition face aux processus visant à collecter des informations sur eux. Cet écart entre les déclarations et les actes est un phénomène ancien qui a été conceptualisé comme le *privacy paradox*.

Jusqu'à présent, le sujet du *privacy paradox* était plutôt traité dans une sphère de spécialistes avec des explications et cadrages théoriques qui se complètent mais qui ne sont pas toujours présentés de manière globale. Avec la mise en place en 2018 du RGPD qui détermine un cadre commun valable pour toute l'Europe, le sujet de la protection des données s'est démocratisé tombant alors dans la sphère publique et devenant un sujet de réactions dans l'opinion publique. Ainsi, les médias informent désormais et régulièrement l'opinion publique sur les erreurs des organisations qui ne suivent pas les engagements demandés pour garantir la protection de la vie privée de leurs clients, employés et interlocuteurs divers. Cette publicisation des problèmes rencontrés et l'affichage imposé des sanctions importantes données à ces organisations, participent à l'intérêt porté aujourd'hui au sujet de la protection des données personnelles. Contribuant à la prise en compte concrète de ce sujet, la législation ayant assorti le règlement d'un ensemble de procédures et d'organismes de soutien, chaque citoyen européen

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

peut maintenant être accompagné par les institutions nationales, telle la CNIL pour la France, pour pouvoir agir plus concrètement face à des pratiques qui ne seraient pas *data privacy friendly*.

Dans ce contexte juridique et socioculturel où le sujet de la protection de la vie privée est (re)mis sur le devant de la scène, l'ambition du projet de recherche Sensibdata est d'avoir comme angle d'analyse la protection des données personnelles au regard des utilisateurs finaux, qu'ils soient des individus ou des organisations. En complément des actions possibles avec le RGPD, le projet se veut un outil pour convaincre de l'intérêt de l'apprentissage d'une hygiène de l'usage du numérique, et diffuser des éléments favorables à la prise de conscience de son importance. La première étape est de montrer en quoi cette hygiène numérique est un sujet important. Ainsi, la sensibilisation aux défis et enjeux de la protection de la vie privée et, par conséquent, la sensibilisation à la maîtrise des données à caractère personnel qui sont diffusées sur les espaces numériques, ont été et restent au cœur des projets présentés et des travaux entrepris et menés par les chercheurs de Sensibdata.

Les travaux de Sensibdata visent à répondre à des ambitions de compréhension intégrée. Ainsi, l'équipe de recherche s'appuie sur une pluralité de regards disciplinaires[1] et de partenaires[2] afin de dépasser de possibles querelles épistémologiques. L'objet de compréhension était les pratiques des utilisateurs, qu'ils

1. *Disciplines* : droit, droit privé, marketing-sciences de gestion, philosophie des sciences sociales et éthique, psychologie sociale, science politique et sciences de l'information et de la communication, sciences de gestion, sciences de gestion-management, sciences de l'information et de la communication, sciences de l'éducation, sciences du langage et sciences de l'éducation, sociologie des techniques.
2. *Partenaires académiques régionaux* : EA 2652 Laboratoire d'économie et gestion de l'ouest (LEGO) ; UMR 6051 ARENES (anciennement Centre de recherches sur l'action politique en Europe – Crape) ; IMT Atlantique, Département systèmes réseaux, cybersécurité et droit du numérique (SRCD) ; EA 1285 Laboratoire de psychologie, cognition, comportement, communication (LP3C) ; EA 7469 Laboratoire Plurilinguismes, représentations, expressions francophones, information, communication, sociolinguistique (PREFICS) ; Équipe Expression (*Expressiveness in human centered data/media*) de l'Institut de recherche en informatique et systèmes aléatoire (IRISA) – UMR CNRS. *Partenaires académiques nationaux* : laboratoire LASCO (Laboratoire sens et compréhension du monde contemporain) de l'Institut Mines-Télécom Business School/université d'Evry Paris Saclay – Équipe de recherche ETHOS (Éthique, technologies, humains, organisations, société) – Équipe « Consommateur connecté dans la société numérique » ; Laboratoire en innovation, technologie, économie et management (LITEM) ; Laboratoire de recherche Audencia-Centrale Nantes (Laboratoire Rn'B Lab) ; Institut des sciences de la communication du CNRS (ISCC) ; Costech (EA2223), Connaissance organisation et systèmes techniques, Laboratoire de recherche du département technologies et sciences de l'homme de l'université de technologie de Compiègne (UTC) ; LabEx ICCA ; Institut de recherche médias, cultures, communication et numérique (Irméccen), EA7546 (Équipe MCPN) ; Industries culturelles et création artistique, université Sorbonne Nouvelle, Paris 3. *Partenaires académiques internationaux* : Academia de studii economice din Bucureşti, Catedra de marketing (Bucarest, Roumanie).

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

soient consommateurs citoyens, ou qu'ils soient responsables de la gestion de la relation au public, afin de pouvoir ensuite établir les fondements permettant de savoir qui, comment et dans quelles limites on peut espérer sensibiliser et responsabiliser les acteurs de l'internet fixe et mobile. Ce projet reste d'actualité et prend toujours plus de sens en prévision du monde à venir où nous vivrons dans un monde toujours plus connecté, en fixe et en mobile, et où fonctionneront de plus en plus systématiquement des objets intelligents (*Internet of things)*.

Répondant à ce projet de contribuer à la sensibilisation à l'hygiène numérique individuelle, cet ouvrage en est l'une des concrétisations. Aussi, nous tenons à remercier chaleureusement tous les auteurs de cet ouvrage collectif d'avoir accepté de consacrer du temps à partager leur précieuse expertise.

Positionnement de l'ouvrage

Cet ouvrage se veut savant du fait de la qualité scientifique des écrits mais aussi résolument orienté grand public pour sa lecture. Dans un contexte médiatique anxiogène sur les données personnelles, les articles courts, et même parfois ludiques pour en favoriser la lecture et dédramatiser le sujet, ont été privilégiés. Le sujet de l'hygiène numérique est pensé selon différents angles. Le lecteur pourra se projeter dans les propos sur les vulnérabilités des individus. Il découvrira, selon la nature de celles-ci, les phénomènes conduisant à leur occurrence. Il pourra s'interroger et évaluer les conditions de la mise en danger de soi induites par certains usages des outils numériques. En considérant toutes les populations ciblées par les stratégies d'incitation au dévoilement de soi, et pas seulement les adolescents ou les personnes peu conscientes des modèles d'affaires qui nécessitent toujours plus de collectes de données, le lecteur comprendra sur quels biais cognitifs et systèmes de pensée, les modèles d'influence et de manipulation peuvent fonctionner pour favoriser la collecte et permettre alors l'exploitation des informations personnelles, qu'elles aient été diffusées par l'utilisateur lui-même, volontairement et en conscience, ou involontairement au sens où l'utilisateur n'a pas eu l'impression d'avoir été clairement informé de cette diffusion. De cette manière, il s'agit aussi de montrer au lecteur que le niveau de risque existant implique des actions variables. Cette partie de la lecture ambitionne aussi de rappeler que le degré de vulnérabilité d'un individu est indépendant de son expérience et de son niveau d'usage des outils numériques. Ayant souligné les mises en dangers et leurs formes variables (manipulations, formes d'attaques, techniques d'ingérence permises par le traitement de données à caractère personnel, utilisations d'informations sur les adresses IP, exploitation des données produites lors de l'usage des objets connectés, etc.), l'ouvrage expose certaines des stratégies individuelles de protection et d'autoprotection disponibles à l'échelle individuelle. Au-delà des techniques connues telles que la falsification des données, l'obfuscation, ou

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

l'utilisation de logiciels antipublicitaires, les actions de maîtrise et de protection de la diffusion des données que chacun doit mener dépendent de la situation individuelle. S'il y a des principes fondateurs et communs, il n'existe pas une bonne hygiène numérique valable pour tous. Il est plus raisonnable de penser l'hygiène numérique comme des principes généraux et des adaptations aux différentes situations et projets individuels. Sans utiliser un vocabulaire technique et en veillant à rendre ces descriptions accessibles pour le grand public, les articles s'y référant se proposent d'être des éclairages sur les conditions et moyens de l'hygiène numérique de l'individu agissant pour son compte ou au sein de son organisation.

Les propos relatifs aux stratégies organisationnelles de sensibilisation et d'accompagnement à la protection des données personnelles répondent, pour leur part, à l'objectif de sensibiliser les lecteurs afin qu'ils se projettent dans des actions à entreprendre et à soutenir au sein de leurs organisations de référence (entreprise, collectivité territoriale, cercle associatif, espace de vie extraprofessionnelle, etc.). L'ambition est alors de contribuer à la démonstration de l'importance d'une action individuelle au sein des collectifs organisationnels.

Organisation de l'ouvrage

Cet ouvrage est organisé de façon à apporter de la connaissance et des propositions d'outils pour sensibiliser citoyens et organisations à une hygiène numérique. Il s'agit pour cela de mieux expliciter le *privacy paradox* dans le contexte actuel d'hyper-connectivité et d'usage du *smartphone*, des réseaux sociaux. L'ambition est de comprendre comment les attentes des utilisateurs en termes de *data privacy* sont modérées par la méconnaissance des menaces qu'ils encourent, annihilées par des contraintes techniques et commerciales, et subordonnées à des comportements dont les citoyens ne perçoivent pas les risques associés. Tout un chacun baigne dans un environnement marqué par une augmentation de la collecte et du traitement de ses données personnelles. L'exemple d'« Une journée type en ligne » donné par la CNIL en 2020 est particulièrement explicite du phénomène des données personnelles en sous-marin de nos journées digitales (CNIL, 2020) :

> « Au lever, vous demandez à votre assistant vocal de vous lire vos derniers courriers électroniques pendant que vous vous habillez pour vous rendre au travail. Dans les transports en commun, vous vous rendez sur une plateforme de *microblogging* avant de consulter un site d'information en ligne renommé. Sur le chemin, vous vous arrêtez prendre une tasse de café et en profitez pour publier une photo de votre petit-déjeuner en « taguant » l'établissement dans lequel vous vous trouvez sur votre réseau social préféré. Durant la pause déjeuner, vous vous rendez sur un site d'e-commerce afin de rechercher une

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

> nouvelle paire de lunettes de ski pour votre week-end à la montagne avant de vous rendre sur votre réseau social pour partager vos plans avec vos amis. Il ne s'agit que d'une poignée de services, mais les données relatives à ces activités et associées à votre profil ont potentiellement été collectées non pas par une dizaine d'acteurs avec lesquels vous avez eu une interaction en ligne mais par plus d'une centaine d'entreprises différentes en l'espace d'une journée.
>
> Si les sites web et les applications avec lesquels vous interagissez sont visibles, d'autres sociétés peuvent suivre vos activités et collecter des données relatives à votre navigation en ligne sans que cela ne soit nécessairement évident pour vous, pour vous afficher de la publicité. Plus tard dans la journée, vous commencez à voir des messages sponsorisés sur votre plateforme de *micro-blogging* à propos de week-ends à la montagne, des annonces publicitaires sur votre réseau social pour les lunettes de ski que vous avez cherchées et des suggestions de nouveaux cafés à découvrir près de votre lieu de travail. Il ne s'agit pas de coïncidences, mais bien du résultat de la collecte de vos données de navigation et de géolocalisation. »

Dans ce cadre, l'ouvrage est organisé selon trois grandes thématiques facilitant le travail de repérage du lecteur mais aussi d'association avec son quotidien digital.

La première partie expose « Les droits à la vie privée et la protection des données personnelles ». Julien Rossi porte un regard historique jusqu'à contemporain sur le droit à la protection des données à caractère personnel. Il montre combien les textes juridiques se caractérisent par leur stabilité et adoptent un paradigme libéral du droit à la vie privée. Celui-ci propose ainsi à l'individu de définir le périmètre de son espace privé par rapport à l'espace public plutôt qu'une définition qui serait édictée par l'État. Romain Gola présente le Règlement général sur la protection des données (RGPD) adopté le 27 avril 2016, mis en application dans tous les États membres en mai 2018, et ses grandes conséquences pour les citoyens et les entreprises. Le RGPD est fondé principalement sur les concepts d'*accountability* (la mise en conformité) et de *privacy by design* (le respect de la vie privée dès la conception des outils numériques). Ce règlement repose sur un pacte social entre les acteurs privés et publics et constitue non pas seulement une contrainte pour les entreprises mais plutôt une opportunité de s'inscrire dans une démarche de corégulation et d'innovation responsable. Annie Blandin examine les modalités d'exercice du droit à la portabilité. Cette dimension juridique fait partie des innovations du RGPD et se caractérise notamment par sa technicité. L'auteure s'interroge sur la facilité d'utilisation de la portabilité par le grand public et le développement de ce droit dans un cadre plus collectif. Sarah Catalan et Lucas Vinit Somolinos constatent que toutes les organisations ne suivent pas le RGPD car il existe un décalage entre la mise en conformité qui est souvent longue et coûteuse, et entre les contrôles de la CNIL

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

qui ne sont pas assez nombreux. Les auteurs appellent à ce que les compétences minimales des Délégués à la protection des données (DPO) soient établies au niveau Européen. Arrah-Marie Jo étudie le cas du marché de la publicité en ligne qui utilise une norme privée pour gérer le consentement. Elle s'interroge au sujet de l'impact des réglementations sur la concurrence dans les *data-driven market*. Sarah Catalan et Lucas Vinit Somolinos soulignent deux immaturités de la version actuelle du RGPD et se penchent sur les problèmes que cette situation engendre. Ainsi, ils relèvent que, premièrement, son volet technique reste imprécis sur les mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel. Deuxièmement, ils notent que le RGPD ne décrit pas les critères permettant la certification d'une organisation, d'un produit ou d'un processus au RGPD, et qu'actuellement cette certification repose uniquement sur un contrôle de la CNIL.

La deuxième partie se penche sur « Les enjeux sociétaux de la protection des données personnelles ». Jean-Sébastien Vayre remet en cause l'idée selon laquelle les nouveaux systèmes de captation sur Internet pour mieux connaître les publics et capter leur attention, dans le cadre des mégadonnées et de l'intelligence artificielle, sont des outils puissants pour manipuler l'opinion, tout en traitant les problèmes sociaux et cognitifs posés par ces nouvelles technologies. À défaut de considérer les internautes comme des êtres crédules et ne sachant pas faire usage de leur raison, il invite à cultiver leur esprit critique afin de limiter la circulation de fausses informations. Jack Noël brosse un tableau synthétique et concret d'histoires de crises cyber utilisant les données personnelles afin d'en tirer des enseignements factuels. Son texte démontre combien les aspects négligence et piratage sont au cœur de l'attention. Ceci ouvre les perspectives sur la collecte « légale », l'exploitation et la monétisation des données personnelles. Loïc Louër montre que l'accès maintenant aisé aux données personnelles facilite grandement le travail de l'espionnage économique. Dès lors, il souligne combien la « surface de vulnérabilité » à l'espionnage économique de toute structure économique (entreprise, laboratoire de recherche, cabinet d'audit…) est augmentée. Conscient de cette vulnérabilité augmentée, chaque individu se doit d'autant plus d'être vigilant pour protéger les actifs stratégiques de son organisation d'appartenance. Dans un deuxième article lié au précédent, Loïc Louër propose une méthode pragmatique permettant d'identifier les données sensibles au sens où leur perte ou leur divulgation présenteraient un préjudice considérable pour l'individu ou son entreprise. Nicolas Béchet et Giuzzeppe Beriot s'intéressent quant à eux au modèle d'apprentissage du risque individuel et collectif. Cette compréhension vise la construction et la mise en place d'un outil de recommandation d'usage automatisé qui pourrait prendre la forme, par exemple, d'une application sur *smartphone* qui émettrait des alertes dès qu'un comportement à risque est décelé. Ils décrivent les trois phases d'opérationnalisation d'un tel modèle : l'analyse manuelle, l'étiquetage des données et finalement la

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

phase d'apprentissage. Florian Hémont cherche à sensibiliser les lecteurs aux enjeux associés à la collecte de données, ainsi que de mettre en avant l'ampleur de celle-ci, à partir d'une étude consistant à recueillir les réactions des utilisateurs à l'exposition d'une partie de leurs données. Stéphane Salvan traite des vulnérabilités intrinsèques à la nature humaine. Il met en avant comment l'utilisation combinée des biais cognitifs et des systèmes de réflexion 1&2, une fois associés dans le contexte du cyberespace, permettent d'influencer les prises de décision des individus. Comme il le souligne, ces biais sont soumis et renforcés par le besoin de dopamine de l'espèce que nous sommes en tant qu'humains. Finalement, Valérie Renault et Arnauld Séjourné présentent la méthodologie de conception d'un jeu sérieux d'évasion et les expérimentations réalisées dans le cadre de ce projet nommé « Camille 2.4.0 ». Ce jeu permet aux adolescents et à leurs parents, cibles prioritaires envisagées, de découvrir comment se crée une identité numérique à partir des traces laissées sur les réseaux sociaux et sur les différents environnements numériques. L'article s'interroge ensuite sur les difficultés de lier gamification et mécaniques de jeu sur des apprentissages ancrés sur des habitudes des usagers dans les environnements numériques.

La troisième partie porte sur « Les organisations face aux données personnelles ». Se penchant sur la notion du niveau de menace, Ksenia Ermoshina et Francesca Musiani notent que le chiffrement de bout-en-bout devient de plus en plus diffus dans les outils de messagerie-solutions qui proposent de cacher ou déguiser les communications privées et les activités en ligne. La conception d'outils renforçant le droit à la vie privée préconise l'identification d'un « modèle de menace » qui sert à obtenir un consensus sur le seuil d'anonymat et de confidentialité approprié à un contexte d'usage particulier. Les auteurs discutent de différents cas d'usage, de situations à bas risque où il n'y a « rien à cacher » jusqu'à des scénarios à haut risque, de guerre ou d'autorité étatique, pour se demander comment les utilisateurs, les consultants en sécurité et les développeurs coconstruisent des modèles de menace, décident quelles données dissimuler, et définissent les modalités de réponse à ces différents niveaux de menaces. Les auteurs démontrent que les oppositions classiques, comme « haut risque » *versus* « bas risque », vie privée *versus* sécurité, doivent être redéfinies dans une approche relationnelle, processuelle et contextuelle. Considérant les échanges de données inter-États, Brunessen Bertrand traite en premier lieu les limites de la protection des données personnelles des citoyens européens induites par les transferts internationaux de données réalisées par les grandes plateformes numériques. Puis, en second lieu, elle revient sur les vulnérabilités du RGPD lorsque les données sont stockées sur le territoire européen. Se penchant sur la position des concepteurs de solutions numériques, Vincent Lefrere et Clara Jean traitent des modèles économiques des applications mobiles. Les auteurs passent d'abord en revue la littérature en économie afin d'étudier les trois stratégies économiques les plus utilisées par les développeurs. Ils s'intéressent ensuite à la

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

manière dont ces différentes stratégies contribuent à la création d'une application à succès. Ils soulignent enfin le rôle des parties tierces dans ces stratégies à travers la commercialisation des applications, avec un focus sur le Google Play Store. Christine Petr et Margot Beauchamps ont identifié cinq postures types des individus sur leur représentation de la collecte des données sur *smartphone*, à partir d'une étude exploratoire. Ces postures pourraient constituer les dimensions de l'attitude par rapport à la collecte des données. Stéphane Salvan s'intéresse aux altérations du processus décisionnel qui sont accentuées par les pratiques des acteurs majeurs du cyberespace. Exploitant une stratégie d'addiction au plaisir d'utilisation des outils et services numériques, le passage du système *pull to push* qui vise à alimenter les internautes en informations sélectionnées pour eux et non pas eux, il argumente sur la stratégie des acteurs du numérique qui mise sur « la paresse intellectuelle » et sur le contrôle de l'accès à l'information qui conduit à une extrême prédictibilité des actions des utilisateurs. Pour finir, Laetitia Della Torre montre comment le RGPD est interprété et appliqué dans le secteur humanitaire et questionne sa position en tant que cadre protecteur. Elle conclut que les NTIC, s'ils permettent une collecte plus précise de données à des fins d'audit et d'évaluation, et impliquent dès lors une gestion et un contrôle plus efficaces des populations en migration, comprennent aussi un certain nombre de vulnérabilités et de risques. Ainsi, le secteur humanitaire n'échappe pas aux fuites de données et *hackings*. Les questions qui se posent sont alors de savoir si leur nature est spécifique au secteur ou s'il s'agit des risques intrinsèquement associés aux usages et outils numériques. Elle note que ces risques sont progressivement pris en compte mais qu'ils ne sont pas encore nécessairement perçus par tous les acteurs du secteur qui ne disposent pas encore d'outils et d'une stratégie éprouvée pour y répondre.

Bibliographie

Agence nationale de la cohésion des territoires, 2021, « Conseillers numériques France Services », [https://agence-cohesion-territoires.gouv.fr/conseillers-numeriques-france-services-437], consulté le 15 juin 2022.

Cnil, 2020, « Publicité ciblée en ligne : quels enjeux pour la protection des données personnelles ? | CNIL », [https://www.cnil.fr/fr/definition/publicite-ciblee], consulté le 15 juin 2022.

Larousse, « hygiène », Dictionnaire de français Larousse, [https://www.larousse.fr/dictionnaires/francais/hygi%C3%A8ne/40927], consulté le 15 juin 2022.

Mattatia Fabrice, 2021, *RGPD et droit des données personnelles*, Paris, Éditions Eyrolles.

Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, 2021, « Inclusion numérique : lancement du recrutement de 4 000 conseillers numériques », [https://www.economie.gouv.fr/plan-de-relance/inclusion-numerique-recrutement-conseillers-numeriques#], consulté le 15 juin 2022.

Pellegrini François, 2019, « Sécurité et hygiène numérique des professionnels », *Dalloz IP/IT*, nº 4, p. 233-236.

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr

Raimondo Laurane, 2021, *La protection des données personnelles en 100 questions/réponses*, Paris, Éditions Ellipses.

Waelbroeck Patrick, Levallois-Barth Catherine, Laurent Maryline et Meseguer Ivan, 2019, Deuxième synthèse du rapport « Données personnelles et confiance : évolution des perceptions et des usages post-RGPD », chaire Valeurs et politiques des informations personnelles, 15 octobre 2019.

« Le droit à la vie privée », Christine Petr et Olivier Segard
ISBN 978-2-7535-9574-3 Presses universitaires de Rennes, 2024, www.pur-editions.fr