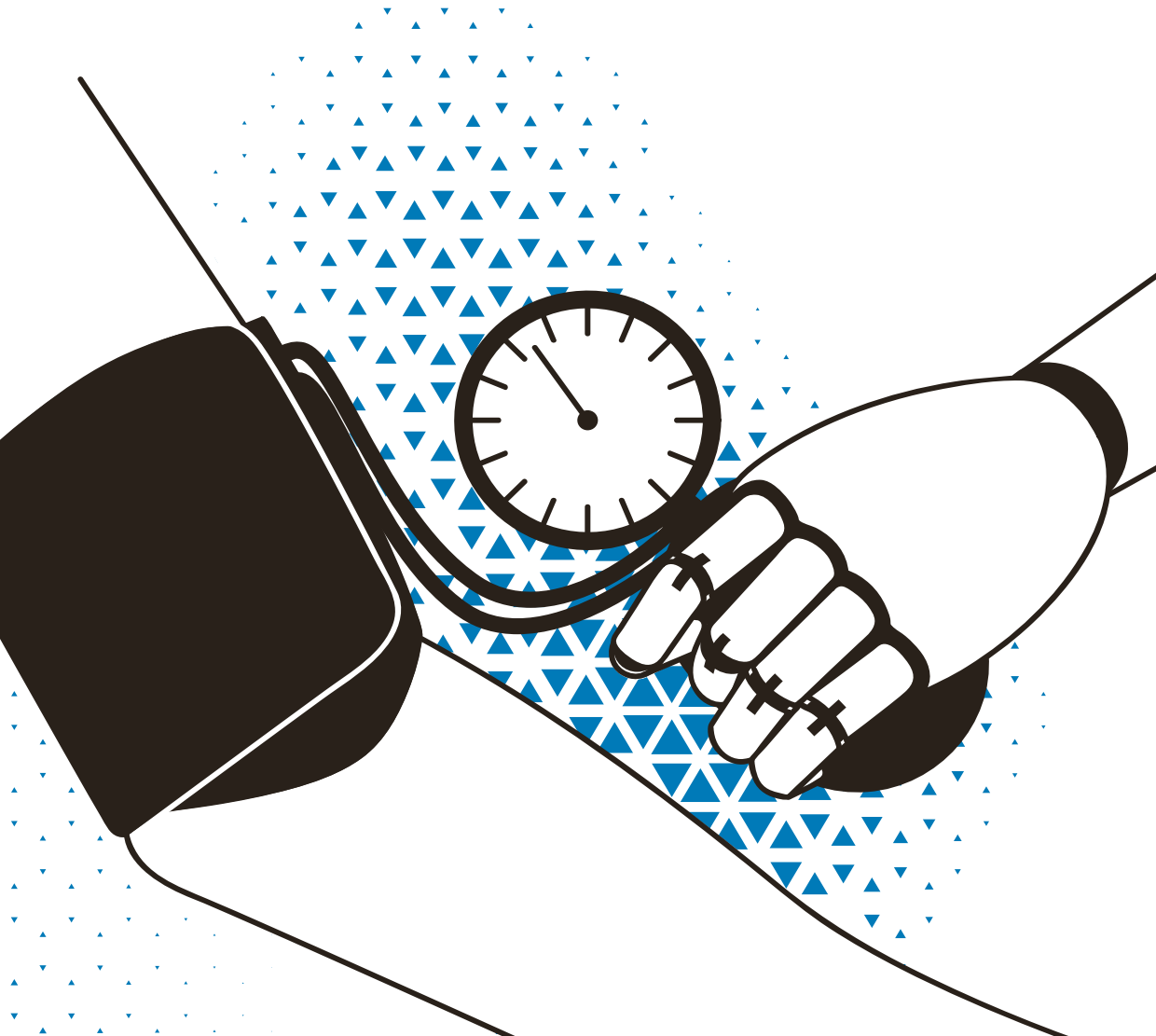
Droits fondamentaux et droits humains à l'ère numérique

Sabrina Ghielmini, Christine Kaufmann, Charlotte Post,
Tina Büchler, Mara Wehrli, Michèle Amacker



Droits fondamentaux et droits humains à l’ère numérique

Sabrina Ghielmini, Christine Kaufmann, Charlotte Post,
Tina Büchler, Mara Wehrli et Michèle Amacker

Éditeur : Centre suisse de compétence pour les droits humains (CSDH)
Responsable du projet : Sabrina Ghielmini
Relecture : Antonia Bertschinger
Réalisation de la couverture et illustrations : buch & netz, Carolina Flores
Maison d'édition et production : buch & netz (buchundnetz.com)

ISBN :
978-3-03805-362-0 (imprimé – broché)
978-3-03805-398-9 (PDF)
978-3-03805-399-6 (EPUB)
978-3-03805-400-9 (Mobi / Kindle)
Version : 1.00-20210414

Cet ouvrage est disponible sous forme de livre en ligne et de livre électronique buch & netz dans différents formats, ainsi que sous forme de livre imprimé. Pour plus d'informations, veuillez consulter l'URL : https://buchundnetz.com/werke/droits-fondamentaux-et-droits-humains-à-l'ère-numérique.

L'édition allemande de l'ouvrage est disponible à l'adresse suivante : https://buchundnetz.com/werke/grund-und-menschenrechte-in-einer-digitalen-welt/.

Cet ouvrage est publié par le Centre suisse de compétence pour les droits humains (CSDH).

La publication du présent ouvrage n'aurait pas été possible sans l'aide financière de la Fondation Hirschmann.
www.hirschmann-stiftung.ch

HIRSCHMANN STIFTUNG

Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Centre suisse de compétence pour les droits humains (CSDH)
Centro svizzero di competenza per i diritti umani (CSDU)
Swiss Centre of Expertise in Human Rights (SCHR)

Table des matières

Deuxième partie
Présentation de cas pratiques

Remerciements

Plusieurs spécialistes ont contribué, par leurs précieuses suggestions, à la réalisation de cet ouvrage. Nous tenons à remercier chaleureusement Sophie Achermann (alliance F), Kathrin Arioli (chancelière du canton de Zurich), Bruno Baeriswyl (ancien préposé à la protection des données du canton de Zurich), Stefanie Becker (Alzheimer Suisse), Abraham Bernstein (Digital Society Initiative, Université de Zurich), Corinna Bath (TU Braunschweig), Nadja Braun Binder (Université de Bâle), Markus Christen (Digital Society Initiative, Université de Zurich), Guy Ehrler (La Poste SA), Alfred Früh (Université de Bâle, auparavant Center for Information Technology, Society and Law, Université de Zurich), Giulia Reimann (Commission fédérale contre le racisme) et Marc Thommen (délégué Open Science, Université de Zurich). Nous remercions aussi Rolf H. Weber (Center for Information Technology, Society and Law, Université de Zurich) pour la révision critique du manuscrit.

Nos remerciements vont également à Res Schuerch (CSDH) et à Moritz Senn (chaire de droit public, droit international et droit européen, Université de Zurich) pour leur soutien lors de la recherche d'informations ainsi qu'à Antonia Bertschinger (CSDH) pour la relecture.

Un grand merci à Nadine Cuennet Perbellini et Jean-François Cuennet, chargés de la traduction allemand-français, et à Claire Robinson (CSDH) pour la relecture.

La réalisation de ce guide n'aurait pas été possible sans la contribution financière de la Fondation Hirschmann, que nous tenons à remercier ici de son généreux soutien et de la confiance qu'elle nous a accordée.

Pour le CSDH

Christine Kaufmann et Michèle Amacker

Préface

Le but des nouvelles technologies devrait être d'une part de nous rendre la vie plus simple et plus facile et, d'autre part, de créer des opportunités. Or, si elles ont assurément cette utilité, elles génèrent aussi des risques et posent de nouveaux enjeux pour notre société : présentes dans tous les aspects de notre vie, elles font surgir toujours plus de questions éthiques, comme dans le domaine de l'intelligence artificielle ou de la robotique. Nos données laissent des traces, et avec elles de nombreuses informations dont nous perdons vite le contrôle. Grâce aux réseaux sociaux, il est maintenant plus facile de réunir des foules, mais aussi de les manipuler et de diffuser de fausses informations. Les exemples du blocage des comptes Twitter de Donald Trump ou des restrictions de l'accès à Internet en Chine ou en Biélorussie attestent de la problématique en matière de liberté d'expression et de réunion ainsi que de l'urgence d'agir dans ce domaine.

Je salue donc cette publication : le monde numérique étant en soi déjà très complexe en raison des avancées constantes de la technologie, il est en effet d'autant plus important de l'analyser à l'aune des droits fondamentaux et des droits humains et d'accompagner son évolution. Les technologies numériques peuvent être d'une grande utilité pour l'humanité, mais comme toute technologie, elles ont autant leur part d'ombre que leurs risques et peuvent être utilisées à mauvais escient. Le monde de la recherche scientifique, appelé à se pencher sur cette problématique, nous donne une orientation, mais pointe aussi du doigt les lacunes de notre cadre juridique.

Cet ouvrage ne fait pas que dresser un tableau de nos droits et libertés fondamentales et de leur sauvegarde dans l'espace numérique, il indique aussi aux pouvoirs publics les aspects qu'ils doivent réglementer. Cette réglementation est en effet nécessaire pour que la population puisse continuer à avoir confiance en notre État de droit. Seuls la protection assurée par ce dernier et les droits qu'il est possible de faire valoir en justice peuvent accroître la confiance dans les nouvelles technologies. Il nous faut donc nous pencher sur cet important nouveau domaine du droit qu'est le cyberespace.

Les droits humains universels s'appliquent en principe tant au monde analogique qu'au monde numérique. Il ne s'agit par conséquent pas de conce-

voir de nouveaux droits ni de revoir la manière de les appliquer et de les interpréter, car ces droits restent valables. La numérisation fait cependant apparaître des questions d'interprétation et de nouveaux domaines d'application, pour lesquels il nous faut des principes, des valeurs à respecter, qui puissent servir de repères aux gouvernements, au secteur privé et à la société civile. Le Groupe de travail de haut niveau des Nations Unies sur la coopération numérique, dont je suis membre, a identifié neuf valeurs humaines qui devraient nous guider dans cette démarche : l'inclusion, le respect, l'humanisme, l'épanouissement individuel, la transparence, la collaboration, l'accessibilité, la durabilité et l'harmonie. Si l'on veut accompagner le développement et l'application de ces technologies numériques, il serait utile que la communauté internationale reconnaisse ces principes, qu'elle s'engage dans une coopération numérique, adopte une vision fondée sur des valeurs et principes communs et se dote d'une nouvelle gouvernance, puisque la numérisation a rendu notre manière de collaborer caduque. L'insécurité, qui restera importante tant que nous ne disposerons pas de normes claires et d'une jurisprudence étoffée sur ces questions, profite aux grandes entreprises technologiques, tandis que l'utilisateur ou l'utilisatrice n'est la plupart du temps pas capable de saisir la justice pour faire respecter ses droits de la personnalité.

Tout porte la Suisse à s'investir dans ce domaine et à montrer la voie : elle a inscrit dans sa Constitution (art. 54, al. 2) son engagement en faveur des droits humains, héritage d'une longue tradition, et accueille dans la Genève internationale un grand nombre d'institutions de référence en la matière. La Suisse tant politique que scientifique se doit donc de s'engager dans cette problématique, de participer à son développement et de s'y investir, aux côtés de l'Union européenne, qui a déjà posé des jalons au retentissement international, notamment avec son règlement relatif à la protection des données. Dans cette perspective, il est indispensable de prendre davantage conscience de l'importance des droits et libertés fondamentales dans notre quotidien numérisé. C'est à cela que cet ouvrage est destiné à contribuer.

Doris Leuthard, ancienne conseillère fédérale

Introduction

La révolution numérique entraîne de profondes transformations dans notre société : il suffit de penser à la robotique, à l'intelligence artificielle, aux mégadonnées et à l'Internet des objets pour s'en convaincre.

Dans les domaines les plus divers, la numérisation peut devenir une précieuse alliée des droits fondamentaux et des droits humains : Internet nous donne accès à des technologies d'information et de communication hors pair ; les robots peuvent résorber la pénurie de personnel soignant et des vêtements intelligents protéger les travailleurs et travailleuses. Toute médaille a cependant son revers : la numérisation est aussi susceptible d'aggraver les violations des droits fondamentaux et des droits humains et d'en faire émerger de nouvelles. La collecte de données personnelles et les outils de surveillance numérique, par exemple, soulèvent des questions relevant notamment du droit au respect de la vie privée et de la liberté de mouvement.

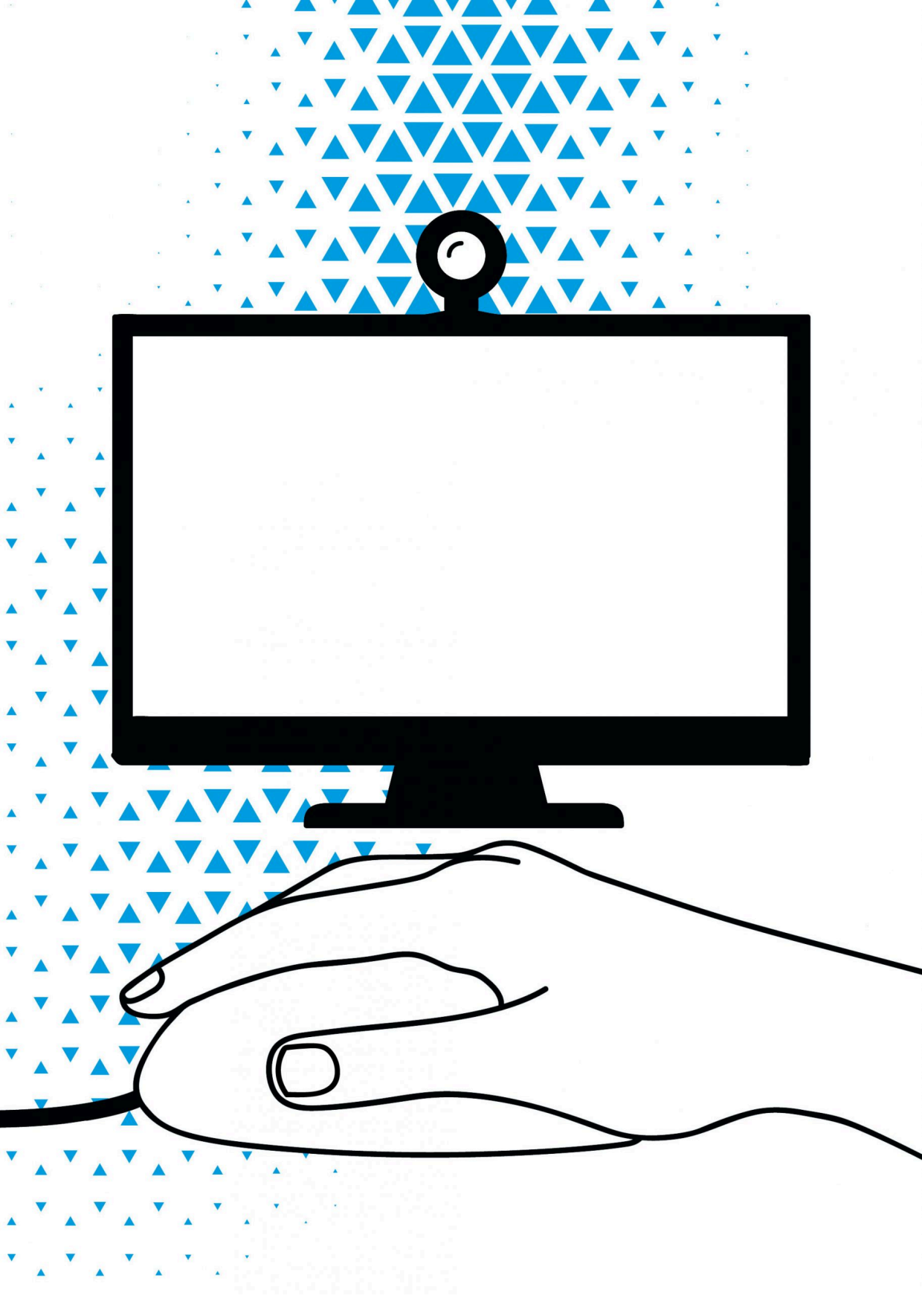
Le présent ouvrage, qui s'adresse à un large public sans connaissances techniques ni juridiques particulières, fait un tour d'horizon des conséquences des technologies numériques pour les droits fondamentaux et les droits humains. Il illustre à l'aide d'exemples dans quels domaines de la vie quotidienne les technologies numériques peuvent porter atteinte aux droits fondamentaux et aux droits humains, ce que l'on peut en dire du point de vue juridique et quelles sont les possibilités de faire valoir ces droits.

Ce livre comprend deux parties. Nous présentons dans la première les principales technologies et leurs applications ainsi que les bases légales en la matière. Dans la seconde, nous illustrons notre propos à l'aide de cas pratiques tirés de divers domaines de la vie. Les technologies numériques ayant d'innombrables applications, nous avons dû opérer un choix. Cet ouvrage ne reflète par conséquent pas tous les domaines de la vie concernés par cette problématique ni toutes les questions juridiques qu'elle soulève. Nous avons en outre simplifié les faits pour les rendre plus facilement compréhensibles, ce qui fait de cet ouvrage un guide pratique, et pas juridique. Les cas pratiques servent à montrer en quoi concrètement les droits fondamentaux et les droits humains sont touchés par l'évolution et les applications des tech-

nologies numériques ; ils ont également pour fonction de nourrir le débat sur la question de la conciliation entre la numérisation et nos droits et libertés fondamentales.

Notre ouvrage reprend en grande partie la structure des trois publications suivantes : *Grund- und Menschenrechte in der Sozialhilfe – Ein Leitfaden für die Praxis* (Droits fondamentaux et droits humains dans l'aide sociale – un guide pratique), *Grund- und Menschenrechte von Menschen mit Behinderungen – Ein Leitfaden für die Praxis der sozialen Arbeit* (Droits fondamentaux et droits humains des personnes en situation de handicap – un guide pratique pour le travail social), tous deux fruits d'une collaboration entre la Haute École de Lucerne et le CSDH, ainsi que l'ouvrage *Droits fondamentaux des personnes âgées – un guide pratique*, publié par le CSDH. Nous tenons par conséquent à en remercier les auteures, Gülcan Akkaya, Eva Maria Belser, Andrea Egbuna-Joss, Sandra Egli, Sabrina Ghielmini, Jasmin Jung-Blattmann et Christine Kaufmann pour le travail de conceptualisation réalisé en amont.

Finalement, une note des traducteurs : par souci de clarté, nous mentionnons également le terme anglais entre parenthèses à la première occurrence des notions pour lesquelles l'usage du terme français ne s'est pas totalement imposé, ou lorsque les deux termes sont utilisés. Et nous mentionnons aussi plusieurs termes lorsque plusieurs expressions françaises coexistent.



Première partie

Notions fondamentales

1 Les technologies numériques et leurs applications

Le tournant sociétal que nous vivons depuis les années 1990, souvent qualifié de « quatrième révolution industrielle », se caractérise par les technologies et infrastructures numériques. Dans ce contexte, on entend par « numérisation » la mutation culturelle, sociale et politique induite par le recours aux nouvelles technologies numériques. Ce phénomène est marqué avant tout par une automatisation toujours plus poussée des domaines les plus divers de la vie – qui vont de la production à la gestion des informations – ainsi que par la connexion entre monde virtuel et monde physique.

Ce chapitre est consacré aux technologies numériques soulevant des enjeux particuliers en matière de droits fondamentaux et de droits humains. Il contient également, pour illustrer ces technologies, divers exemples d'application.

1.1 Données, métadonnées et mégadonnées

Les données, en tant qu'informations stockées, existaient déjà avant la numérisation. La nouveauté, c'est que les technologies numériques permettent de stocker ces données sur divers supports. Actuellement, quand on parle de « données », on entend d'une part les informations enregistrées sur un dispositif, qui ont été saisies sur la base d'observations ou de mesures et peuvent être modifiées, traitées ou chiffrées[1] ; et d'autre part les métadonnées, c'est-à-dire les informations sur les caractéristiques d'autres données telles que la date de parution d'un texte ou la date de sa dernière modification. Et l'on qualifie de « données secondaires » les métadonnées fournissant des informations sur les communications réalisées sur Internet, comme la date d'envoi d'un courriel et son destinataire[2].

Une autre notion qui apparaît fréquemment quand il s'agit de numérisation est celle de mégadonnées (*big data*), qui désigne de gigantesques volumes

1 Hattenhauer, Computerlexikon, 2019, p. 98 s. ; Weber, Laux et Oertly, Datenpolitik, 2016, p. 10 s.

2 PFPDT, Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée), 2013, p. 4.

de données non structurées ou semi-structurées. Les technologies actuelles permettent d'analyser de telles masses de données de façon bien plus rapide et plus efficiente qu'il y a quelques années seulement[3].

Les mégadonnées, que les entreprises récoltent par exemple en proposant des applications gratuites à leurs clients en échange du droit d'accéder à leurs données, présentent quatre caractéristiques principales. Elles sont très volumineuses, très hétérogènes, correctes et analysées à une vitesse extrêmement élevée. L'essor des mégadonnées s'explique surtout par l'Internet des objets (*Internet of Things* → **notions fondamentales point 1.5**), qui lui fournit les données, et par l'informatique en nuage (*cloud computing* → **notions fondamentales point 1.6**), qui lui fournit les outils nécessaires à leur traitement[4].

Exemples d'application :

Recherche médicale et diagnostics : la médecine recourt à des données sur l'état de santé des patient·e·s afin de garantir les meilleurs soins possibles. Dans ce domaine, c'est surtout l'informatique biomédicale qui joue un rôle important : à l'aide d'algorithmes (→ **notions fondamentales point 1.2**), les professionnel·le·s analysent les données collectées dans le but de déterminer les thérapies les plus prometteuses ou les caractéristiques génétiques prédisposant à certaines maladies déterminées[5]. Pour être capables d'établir des diagnostics, des logiciels passent en revue d'importants volumes de données afin d'y déceler des caractéristiques en tout genre. Lorsque ces dernières sont présentes dans certaines combinaisons bien précises, le logiciel propose un diagnostic en appliquant des algorithmes. Ces algorithmes opèrent par exemple sur la base d'enregistrements d'appareils médicaux ou de résultats d'analyses de laboratoire qu'ils attribuent à un diagnostic déterminé et donc à une maladie déterminée[6] (→ **cas pratique Diagnostics fondés sur l'intelligence artificielle et les mégadonnées 2.2**).

Microciblage : le microciblage (*microtargeting*) est une méthode utilisée tant en marketing que dans les campagnes électorales et de votations. En exploitant en amont d'importantes quantités de données, on parvient à s'adresser de manière

3 Weber et Thouvenin, Big Data und Datenschutz, 2014, p. 1.
4 Hattenhauer, Computerlexikon, 2019, p. 101.
5 Jiang, Jiang, Zhi et al., Artificial intelligence in healthcare, 2017, p. 230 s.
6 Jiang, Jiang, Zhi et al., Artificial intelligence in healthcare, 2017, p. 230 ; pour un approfondissement, notamment sur le droit de la protection des données : Wirth, Johns, Meurers et al., Anonymisierung medizinscher Daten, 2020, p. 74.

ciblée à des personnes précises. On définit dans ce but des groupes cibles, avant d'établir pour chacun d'eux des profils de personnalité. Des partis politiques, par exemple, font comparer et recouper les données récoltées lors de contacts privés et par des sites internet avec les données de réseaux sociaux afin d'établir des correspondances (appariement, ou *social match*). Cette technique leur permet d'adapter leurs messages politiques en fonction de groupes cibles déterminés et, par exemple, de promouvoir des projets politiques en diffusant des messages « sur mesure » sur les réseaux sociaux[7] (→ **cas pratique Microciblage durant des campagnes politiques 3.4**).

1.2 Algorithmes

Un algorithme est une suite définie d'étapes permettant de résoudre un problème. Un algorithme qui reçoit les mêmes données de départ, introduites dans le même ordre, suivra systématiquement les mêmes étapes prédéfinies, et parviendra donc toujours aux mêmes résultats ; si, en revanche, les données de départ ne sont pas les mêmes, il parviendra à des résultats différents[8]. De cette manière, les algorithmes permettent de rechercher une caractéristique prédéfinie dans toutes sortes de jeux de données ou d'obtenir toujours les mêmes résultats si l'on entre les mêmes données dans un moteur de recherche[9].

Exemples d'application :

Bulles de filtres : les internautes peuvent se retrouver dans des bulles informationnelles, ou bulles de filtres (*filter bubble*), ou encore chambres d'écho, car ils ne voient souvent s'afficher que de la publicité ou des informations qui reflètent leurs intérêts ou leurs opinions. Des personnes aux idées politiques conservatrices par exemple se verront plutôt proposer des contenus diffusés par des partis ou des journaux conservateurs. Les internautes sont par conséquent de moins en moins exposés à des opinions différentes des leurs. Ces bulles de filtres se créent parce que les exploitants de moteurs de recherche utilisent des algorithmes qui se fondent entre autres sur les activités antérieures de l'internaute, et notamment sur ses recherches. Ils supposent en effet que les individus préfèrent les contenus qui les confortent dans leurs convictions[10].

7 PFPDT et Privatim, Guide relatif aux élections et votations, 2019, p. 6 s.
8 Hattenhauer, Computerlexikon, 2019, p. 17.
9 Bitkom e.V. et DKFI, Künstliche Intelligenz, 2017, p. 67 s. et 71 s.
10 Bezemek, Filter Bubble and Human Rights, 2020, p. 34 ss.

Calcul de risque : les assurances et les banques peuvent se servir d'algorithmes pour décider de conclure ou non un contrat d'assurance ou d'accorder un crédit. Ces algorithmes sont établis de manière à faire correspondre certaines caractéristiques des client·e·s avec certaines conditions à remplir pour pouvoir conclure une police d'assurance ou obtenir un crédit[11].

Système de recherche automatisée de véhicules : en Suisse, cette technique est appliquée à l'aide du programme « Système de recherche automatisée de véhicules et de surveillance du trafic (RVS) ». Un scanner mobile relève les numéros d'immatriculation et les compare avec ceux enregistrés dans la banque de données de recherche. Lorsque ces numéros coïncident, la police peut faire arrêter le véhicule en question et le contrôler[12].

1.3 Apprentissage automatique

Par apprentissage automatique, ou apprentissage machine, on entend le fait de programmer un algorithme de manière à ce qu'il soit capable d'identifier certains schémas dans des données et d'y « réagir » en fonction de paramètres prédéfinis. Pour ce faire, on alimente le système avec des données contenant une ou plusieurs caractéristiques communes, ce que l'on appelle un « jeu de données d'entraînement »[13]. Lorsque l'algorithme reconnaît la caractéristique en question dans un nouveau jeu de données, il classe automatiquement ce jeu dans le groupe des données présentant cette caractéristique[14]. Ce qu'il a appris grâce au jeu de données d'entraînement le rend donc capable de faire des prédictions[15].

L'apprentissage automatique comprend également un processus encore plus complexe, l'apprentissage profond (*deep learning*), qui consiste à créer des réseaux de neurones artificielles qui s'inspirent des structures fondamentales du cerveau humain. Ces neurones sont capables de fonctionner de manière autonome pour établir des connexions entre elles et traiter des informations et, par conséquent, le système suit des étapes qui échappent

11 Sprecher, Datenschutzrecht und Big Data, 2018, p. 519 ss; Raso, Hilligoss, Krishnamurthy et al., Artificial Intelligence & Human Rights, 2018, p. 26 ss.

12 Arrêt 6B_908/2018 du 7 octobre 2019 du Tribunal fédéral, consid. 2.1 ; SRF, Aargauer und Solothurner Polizei bleiben beim Autonummern-Scanner, 2019.

13 Bitkom e.V. et DKFI, Künstliche Intelligenz, 2017, p. 27.

14 Hattenhauer, Computerlexikon, 2019, p. 220 s.

15 SEFRI, Intelligence artificielle, 2019, p. 20.

souvent à leurs concepteurs et conceptrices. Ces derniers ne peuvent plus savoir sur quoi s'est fondé l'algorithme pour parvenir à ses résultats. C'est ce que l'on appelle l'effet boîte noire[16].

Exemples d'application :

Applications d'activité physique : les apps de sport téléchargent dans un nuage (→ **notions fondamentales point 1.6**) les informations qu'elles tirent du comportement de leurs utilisateurs et utilisatrices. Sur cette base (qui constitue dans ce cas le jeu de données d'entraînement), un algorithme fait des propositions d'activité physique personnalisées.

Véhicules autonomes : afin d'entraîner un programme destiné à piloter un véhicule de manière autonome au milieu du trafic, une personne conduit un véhicule autonome un certain temps afin que l'algorithme puisse reprendre son comportement[17].

1.4 Intelligence artificielle

On parle d'intelligence artificielle (IA) quand des systèmes sont capables d'analyser leur environnement et d'agir avec un certain degré d'autonomie afin d'atteindre des objectifs déterminés. Ces systèmes sont donc créés pour « imiter » l'esprit humain. L'IA peut être utilisée tant dans des systèmes logiciels (assistants vocaux ou moteurs de recherche, par ex.) que dans des systèmes matériels (robots ou véhicules hautement technologiques, par ex.)[18]. Cette définition de l'intelligence artificielle étant très générale, il est utile de souligner trois compétences essentielles présentes dans la plupart des systèmes actuels d'IA :

- capacité d'exploiter de gros volumes de données complexes, comme aucune autre technologie n'a pu le faire auparavant ;
- capacité de faire, en fonction de ces données, des prédictions qui pourront servir de base de décision ;
- capacité d'agir en fonction de ces prédictions.

16 Vallone, Wenn sich Algorithmen absprechen, 2018, p. 37 s. et 45.
17 Bitkom e.V. et DKFI, Künstliche Intelligenz, 2017, p. 27.
18 Commission européenne, L'intelligence artificielle pour l'Europe, 2018, p. 1.

Au centre de l'intelligence artificielle, on trouve donc notamment la capacité de comprendre des processus et d'apprendre de manière autonome[19]. L'une des principales méthodes pour ce faire est l'apprentissage automatique (→ **notions fondamentales point 1.3**)[20].

Exemples d'application :

Assistants vocaux : les assistants vocaux (*chatbots*), sont des robots capables de communiquer en langage naturel avec des êtres humains. Ils sont souvent utilisés afin de fournir à des utilisateurs et utilisatrices une manière simple d'obtenir des renseignements ou des réponses à leurs questions. L'apprentissage automatique joue un rôle important dans leur manière de fonctionner : il permet en effet aux assistants vocaux d'acquérir les compétences requises pour analyser la question qui leur est posée, dégager les intentions des utilisateurs et utilisatrices de leurs propos et, finalement, réaliser des recherches de manière autonome dans des banques de données numériques afin de fournir une réponse satisfaisante[21]. Certains assistants vocaux sont aussi programmés pour apprendre la manière de parler de leurs utilisateurs et utilisatrices, et peuvent donc se mettre à les injurier s'ils ont au préalable été « alimentés » de propos orduriers[22].

Reconnaissance faciale à l'aide de logiciels intelligents : la reconnaissance faciale peut être utilisée de deux manières. D'une part, elle permet de s'assurer qu'une personne est bien autorisée à effectuer une action déterminée (entrer dans un pays, déverrouiller un smartphone ou pénétrer dans un bâtiment, par ex.). D'autre part, elle sert aussi à identifier des individus jusque-là inconnus. Un logiciel de reconnaissance faciale permet notamment de trouver des personnes soupçonnées d'avoir commis un délit : la police saisit la photographie d'une personne inconnue dans le logiciel, qui la compare avec celles d'une banque de données dans laquelle sont enregistrées des photographies d'individus et leur identité. La reconnaissance faciale recourt par conséquent à deux éléments : un logiciel capable de saisir des visages et de les analyser et une banque de données qui permet de comparer les visages de personnes jusque-là inconnues (→ **cas pratiques Vidéosurveillance étatique avec reconnaissance faciale dans l'espace public 3.5** et **Magasin automatique 6.1**).

19 SEFRI, Intelligence artificielle, 2019, p. 7.
20 Bitkom e.V. et DKFI, Künstliche Intelligenz, 2017, p. 32.
21 Bitkom e.V. et DKFI, Künstliche Intelligenz, 2017, p. 44 s.
22 Zeit Online, Twitter-Nutzer machen Chatbot zur Rassistin, 2016.

1.5 Internet des objets

L'Internet des objets (IdO, ou *Internet of Things*), c'est l'interconnexion toujours plus poussée, par le biais d'Internet, d'objets de toutes sortes, qui sont munis de puces et dotés d'un identifiant numérique. Il peut s'agir par exemple de véhicules, d'appareils électroménagers ou d'outils[23]. Cette connexion permet de collecter les données de ces objets et de les transmettre à d'autres objets[24]. Les objets communiquent par conséquent de manière autonome entre eux et réalisent des tâches sans que leur propriétaire n'ait à intervenir de quelque manière que ce soit.

Exemples d'application :

Maison intelligente : une maison intelligente est un logement dont les installations techniques et les appareils électroménagers sont connectés entre eux et parfois, mais pas toujours, à Internet. Des capteurs ou des moteurs sont intégrés à ces appareils, que les utilisateurs et utilisatrices peuvent piloter au moyen d'une application ou d'un assistant vocal. D'un mouvement du doigt ou en donnant un ordre à haute voix, ils allument ou éteignent la lumière, la télévision ou le système d'alarme. Une maison intelligente peut aussi disposer de réfrigérateurs intelligents capables notamment d'enregistrer les denrées prélevées et d'en faire une liste d'achats[25].

Technologie portable : par technologie portable (*wearables*), on entend des appareils que les utilisateurs et utilisatrices portent sur eux ou qui sont intégrés dans les vêtements. Ces appareils peuvent par exemple saisir et analyser des informations sur le type et la fréquence des mouvements, sur la fréquence cardiaque ou sur le sommeil[26] (→ **cas pratiques Surveillance au travail 1.3** et **Capteur d'activité physique d'une caisse-maladie 2.3**).

1.6 Informatique en nuage

L'informatique en nuage, ou informatique dématérialisée (ou encore *cloud computing*) est la possibilité de télécharger les données d'un ordinateur sur

23 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, p. 28. La prochaine étape de l'Internet des objets, c'est l'Internet du tout et l'Internet des corps.

24 OCDE, Going Digital, 2019, p. 19.

25 Eggen, Home Smart Home, 2016, p. 1131 s.

26 Eggen et Stengel, Wearables, 2018, ch. marg. 4 ss.

un serveur décentralisé accessible du monde entier. Le principal avantage, pour les utilisateurs et utilisatrices, est de pouvoir accéder à leurs données de partout, où qu'ils se trouvent[27]. L'informatique en nuage est souvent utilisée pour permettre à plusieurs personnes d'avoir accès de manière décentralisée à des technologies de l'information ou de la communication[28].

Exemples d'application :

Services de flux : pour offrir des services de flux (*streaming*), des entreprises telles que Netflix, Spotify ou Amazon Prime stockent de manière décentralisée de nombreux fichiers (souvent des films ou de la musique), que les utilisateurs et utilisatrices peuvent visualiser directement sur leur dispositif[29].

Services de stockage en nuage : les services de stockage tels que Google Drive, Amazon Cloud ou Microsoft One Drive ont été développés pour faciliter le travail en groupe sur des projets. Ils offrent la possibilité de télécharger de manière décentralisée des données sur un serveur (le nuage, ou *cloud*) et de les rendre accessibles via Internet aux autres membres du groupe[30]. Ils ne sont toutefois pas sans danger, puisque les utilisateurs et utilisatrices risquent de perdre la maîtrise de leurs données et que la protection et la confidentialité des données peuvent ne pas être respectées (un risque particulièrement sérieux pour certaines catégories professionnelles telles que les avocat·e·s, le domaine de la santé et des secteurs régulés comme les marchés financiers). Il n'est par exemple souvent pas facile pour la clientèle de ces services de savoir où se trouve exactement le serveur sur lequel leurs données ont été sauvegardées, ou si le service de stockage les a confiées à des sous-traitants. De plus, étant donné qu'un même système enregistre et traite les données de nombreuses personnes, il suffit que l'une d'entre elles soit victime d'une attaque de hackers (pirate informatique) pour que toutes soient touchées, étant donné que tout le système sera concerné[31].

1.7 Robotique

La robotique désigne des systèmes d'intelligence artificielle qui, souvent, prennent la forme de machines et d'appareils capables de se déplacer. Les

27 Hattenhauer, Computerlexikon, 2019, p. 318.
28 OCDE, Going Digital, 2019, p. 19 s.
29 Hattenhauer, Computerlexikon, 2019, p. 360.
30 Hattenhauer, Computerlexikon, 2019, p. 78 s.
31 PFPDT, Explications concernant l'informatique en nuage (cloud computing), non daté.

robots accomplissent des tâches dangereuses, fatigantes ou monotones pour les êtres humains, et le font souvent de manière plus précise qu'eux. Leur présence fait toutefois augmenter le risque de suppression d'emplois dans diverses branches, puisqu'ils peuvent remplacer du personnel.

Exemples d'application :

Robots sur une chaîne de montage : les robots sont particulièrement adaptés pour effectuer des tâches standardisables. Ils sont programmés de manière à s'acquitter toujours des mêmes opérations, et dans le même ordre[32].

Robots de soins : il existe trois types de robots de soins. Les robots de service peuvent se charger de déplacer de petits objets pour les personnes nécessitant des soins ; les robots d'assistance aident le personnel soignant à déplacer ou à lever des patient·e·s. Quant aux robots de divertissement, ils ont pour tâche de distraire ou de faire bouger des personnes (fonction psychique et physique) ; dotés de capteurs qui perçoivent les mouvements et les contacts physiques, ils sont capables de réagir au comportement de la personne prise en charge[33] (→ **cas pratique Robots de soins 2.1**).

1.8 Chaîne de blocs

Une chaîne de blocs (*blockchain*) est une chaîne formée de blocs de données qui, ensemble, forment une structure de données décentralisée. L'objectif est de pouvoir garantir la sécurité et la traçabilité des transactions, en créant des transactions indépendantes les unes des autres. Techniquement, on y parvient en rendant la signature électronique obligatoire à chaque transaction et en rajoutant pour chaque nouvelle transaction un bloc à la fin de la chaîne de données. Ce processus génère une sorte de registre électronique dans lequel chaque transaction est stockée dans un ordre chronologique précis. La chaîne de blocs a pour particularité que cet ordre ne peut pas être modifié[34]. Elle présente l'avantage d'être gérée de manière décentralisée : la base de données n'est pas stockée sur un seul et unique serveur. Chaque ordinateur participant au réseau stocke lui aussi des copies de la base de données concernée par une transaction. La chaîne de blocs

32 Hattenhauer, Computerlexikon, 2019, p. 318 s.
33 Kreis, Pflegeroboter, 2018, p. 224 s.
34 Weber, Blockchain, 2017, ch. marg. 1.

est par conséquent inviolable, puisqu'il faudrait hacker d'innombrables ordinateurs pour la manipuler. L'accès des individus au protocole est géré par un logiciel d'accès[35]. Les nouveaux évènements ou transactions sont stockées automatiquement et peuvent donc être connus de tous les participant·e·s. Toute tentative de modifier les informations produit une interruption des informations stockées, visible sur tous les serveurs. Les applications de chaînes de blocs les plus connues sont les monnaies virtuelles (Bitcoin, Ether, Ripple, etc.) et les contrats autonomes (*smart contracts*). Quant à l'utilisation de chaînes de blocs pour suivre les produits le long des filières de production, elle est moins connue, mais très importante en pratique[36].

Exemple d'application :

Suivi des filières de production et de distribution : la numérisation intégrale d'un processus de distribution peut aider à mieux gérer les informations sur les biens et à les rendre plus transparentes. Cette technologie est notamment utile pour assurer le respect de normes sociales et écologiques. Un bon exemple de ce type d'application est le marquage d'une espèce de poisson, la légine australe, par une entreprise de pêche australienne : immédiatement après les avoir pêchés, on implante dans les poissons une puce qui enregistrera les informations lors de chaque nouvelle opération. Le lieu de la pêche et les responsables de l'embarcation y seront par exemple saisis. Les informations enregistrées sont codées au moyen de la technologie de chaîne de blocs, ce qui les protège des manipulations. À la fin de la filière, les données sont transférées dans un code QR que les consommateurs peuvent scanner pour connaître l'origine du poisson[37].

35 Hattenhauer, Computerlexikon, 2019, p. 59 ss.

36 OCDE, Blockchain in responsible supply chains, 2019.

37 FAZ Online, Blockchain für den Schwarzen Seehecht, 2019.

2 Droits fondamentaux et droits humains

Les droits fondamentaux et les droits humains, qui réglementent les aspects essentiels de la vie, visent à garantir une existence digne. Les droits fondamentaux désignent généralement les garanties inscrites dans la Constitution fédérale ou dans les constitutions cantonales, tandis que la notion de droits humains se réfère aux droits consacrés à l'échelon supranational, principalement dans des conventions internationales[38]. En Suisse, droits fondamentaux et droits humains instaurent plus ou moins les mêmes droits.

Ce chapitre est divisé en trois parties. La première aborde les enjeux posés par la numérisation en matière de droits fondamentaux et de droits humains (**2.1**), la deuxième passe en revue les principales bases juridiques (**2.2**) et la troisième (**2.3**) présente les caractéristiques essentielles de certains droits fondamentaux et droits humains ainsi que leurs liens avec la numérisation.

2.1 Enjeux posés par la numérisation en matière de droits fondamentaux et de droits humains

Les progrès constants de la numérisation exercent une énorme influence sur la vie en société et entraînent des changements de nature aussi bien culturelle et sociale que politique, économique et écologique. Étant donné qu'ils permettent l'exploitation d'immenses volumes de données et le recours à l'intelligence artificielle, ils n'épargnent aucun domaine de notre existence[39].

Les nouvelles technologies peuvent consolider les droits fondamentaux et les droits humains. Par exemple, les réseaux sociaux favorisent dans certains cas la participation à la vie de la société, l'accès à l'information et la liberté d'expression. Grâce à eux, il devient aussi plus facile de suivre des cours et de participer à des activités culturelles. Toutefois, la numérisation ne comporte pas que des avantages, mais aussi des risques pour nos droits, puisqu'elle permet la surveillance massive, la censure et une collecte prati-

38 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 1, ch. marg. 26.
39 Deutscher Bundestag, Menschenrechte im digitalen Zeitalter, 2018, p. 5.

quement illimitée de données personnelles. En outre, avec l'essor de la numérisation, les personnes sans accès aux nouvelles technologies peuvent être exclues de progrès décisifs, ce qui aggrave la fracture numérique[40].

Il incombe en particulier aux États de réagir face à ces risques. Ils ont en effet la double obligation de respecter les droits fondamentaux et les droits humains et de les préserver de toute atteinte, également dans le domaine de la numérisation, dont les progrès vertigineux interpellent sans cesse quant à la manière de protéger les individus des effets négatifs des nouvelles technologies sur leurs droits. La société a par ailleurs intérêt à utiliser ces technologies de la façon la plus efficiente possible[41]. Conscient lui aussi que la numérisation bouleverse notre façon de vivre en société, le Conseil fédéral a adopté en 2020 la « Stratégie Suisse numérique » qui consacre deux grands principes : la personne humaine doit être au centre de l'évolution numérique et les droits de chaque individu doivent être garantis[42].

Si les droits fondamentaux et les droits humains sont valables dans le monde numérique aussi bien que dans l'analogique, les progrès de la numérisation font cependant apparaître de nouveaux enjeux. En premier lieu, du fait que la plupart des conventions internationales et des catalogues de droits fondamentaux figurant dans les constitutions nationales datent de l'ère analogique, ils n'ont pas, à l'origine, été rédigés pour résoudre des questions liées aux processus numériques. L'essor des réseaux sociaux soulève par exemple une question inédite : la liberté d'opinion s'applique-t-elle aux *tweets* ? Il est par conséquent nécessaire d'adapter les stratégies de protection des droits fondamentaux et des droits humains à l'évolution de la société et de les réinterpréter afin qu'elles abordent également les problèmes posés par la numérisation[43].

Une autre difficulté qui surgit en lien avec les droits fondamentaux et les droits humains dans l'univers du numérique tient au statut des acteurs en présence. En effet, les technologies sont conçues presque exclusivement par des entités privées, qui ont une grande marge de manœuvre pour décider ce qui sera développé, et quelles règles fixer pour l'utilisation de leurs services

40 Haut-Commissariat des Nations Unies aux droits de l'homme, Human Rights in a New Era, 2018.

41 Weber, Digitalisierung, 2019, p. 4.

42 Conseil fédéral, Stratégie Suisse numérique, 2020, p. 4 ss.

43 Weber, Digitalisierung, 2019, p. 5.

et technologies. Pour bien des aspects, l'État n'adopte en effet ni dispositions légales ni consignes. En outre, il arrive fréquemment que les entreprises en question disposent d'une expertise plus pointue que les services publics responsables d'une question donnée. Tout cela confère au secteur privé une influence considérable sur le domaine numérique, et souvent une longueur d'avance sur l'État[44].

Cette situation pose problème, car les entreprises ne sont pas directement liées par les droits fondamentaux et les droits humains, qui créent plutôt des obligations pour l'État et pour les privés assumant une tâche de l'État (art. 35, al. 2, Cst.). Dès lors, les personnes dont les droits sont lésés par des entreprises privées ne peuvent pas faire valoir directement les droits fondamentaux et les droits humains pour obtenir justice. Pour cette raison, un débat a lieu aux échelons national et international sur la nécessité d'instaurer un mécanisme pour amener ou contraindre les entreprises à respecter ces droits ainsi que sur ses modalités[45].

Les États ont, en vertu des conventions internationales et de leurs constitutions, l'obligation de protéger les individus et les entreprises privées contre toute atteinte, par d'autres personnes privées, à leurs droits fondamentaux et à leurs droits humains (*obligation de protection* → **notions fondamentales point 2.2.5**). À cet effet, ils se dotent par exemple de lois sur la protection des données ou contre les atteintes à la personnalité. Il leur est toutefois difficile de concrétiser cette obligation dans le domaine de la numérisation : d'une part, le développement de la législation ne parvient pas à suivre le rythme des progrès technologiques, d'autre part, les processus numériques sont souvent transfrontaliers. Ainsi, à titre d'exemple, les réseaux sociaux unissent des personnes de pays les plus divers, ce qui rend difficile la réglementation de ces réseaux à l'échelon national[46].

44 Jørgensen, Private Actors in the Online Domain, 2018, p. 244 ss.

45 Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme sont un particulièrement bon exemple de cette démarche. Pour de plus amples explications, voir Kälin et Künzli, Menschenrechtsschutz, 2019, p. 91 ss.

46 Jørgensen, Private Actors in the Online Domain, 2018, p. 268.

2.2 Bases juridiques

2.2.1 Quels sont les droits fondamentaux et les droits humains et quels textes les garantissent ?

La Constitution fédérale suisse et la plupart des constitutions cantonales énumèrent les droits fondamentaux de façon détaillée. L'article 41 de la Constitution fédérale contient par ailleurs une liste de sept buts sociaux (sécurité sociale, soins de santé, travail et logement approprié, formation et protection des familles ainsi que promotion et soutien des enfants et des jeunes), dont la teneur est certes inspirée de divers droits humains, mais que l'on ne peut pas invoquer en justice, contrairement aux droits fondamentaux (→ **notions fondamentales point 2.2.4**). Quant aux principales sources de droit internationales pour la Suisse, ce sont la Convention européenne des droits de l'homme (CEDH), le Pacte international relatif aux droits économiques, sociaux et culturels (Pacte social des Nations Unies) et le Pacte international relatif aux droits civils et politiques (Pacte civil des Nations Unies).

La teneur des droits fondamentaux inscrits dans la Constitution fédérale coïncide dans une large mesure avec celle des droits humains, comme il ressort des tableaux ci-dessous, qui présentent les garanties de la Constitution fédérale, de la CEDH et des Pactes des Nations Unies.

Principes de base	
Dignité humaine	art. 7 Cst.
Égalité devant la loi	art. 8, al. 1, Cst., art. 26 Pacte civil de l'ONU
Interdiction de la discrimination	art. 8, al. 2, Cst., art. 14 CEDH, art. 2, al. 1 et art. 26 Pacte civil de l'ONU, art. 2, al. 2, Pacte social de l'ONU
Égalité en droit entre femmes et hommes	art. 8, al. 3, Cst., art. 7 Pacte social de l'ONU
Égalité pour les personnes handicapées	art. 8, al. 4, Cst.
Protection des enfants et des jeunes	art. 11 Cst., art. 24 Pacte civil de l'ONU, art. 10 Pacte social de l'ONU
Protection des minorités	art. 27 Pacte civil de l'ONU
Droit à la reconnaissance de la personnalité juridique	art. 16 Pacte civil de l'ONU
Interdiction de la propagande en faveur de la guerre et de l'incitation à la haine	art. 20 Pacte civil de l'ONU

Protection de l'intégrité physique et psychique ainsi que de la santé	
Droit à la vie	art. 10, al. 1, Cst., art. 2 CEDH, art. 6 Pacte civil de l'ONU
Droit à l'intégrité physique et psychique	art. 10, al. 2, Cst.
Interdiction de la torture et autres peines ou traitements cruels, inhumains ou dégradants	art. 10, al. 3, Cst., Art. 3 CEDH, art. 7 Pacte civil de l'ONU
Droit à la liberté personnelle	art. 10, al. 2, Cst.
Liberté de mouvement	art. 10, al. 2, Cst., art. 12, al. 1, Pacte civil de l'ONU
Liberté d'établissement	art. 24 Cst., art. 12 Pacte civil de l'ONU
Droit à la santé	art. 12 Pacte social de l'ONU
Protection contre l'expulsion, l'extradition et le refoulement	art. 25 Cst., art. 13 Pacte civil de l'ONU

Opinions, convictions et communication	
Liberté de conscience et de croyance	art. 15 Cst., art. 9 CEDH, art. 18 Pacte civil de l'ONU
Liberté d'opinion et d'information	art. 16 Cst., art. 10 CEDH, art. 19 Pacte civil de l'ONU
Liberté des médias	art. 17 Cst., art. 10 CEDH, art. 19 Pacte civil de l'ONU
Liberté de la langue	art. 18 Cst.
Liberté de l'art	art. 21 Cst., art. 15 Pacte social de l'ONU
Droit de participer à la vie culturelle	art. 15, al. 1, let. a, Pacte social de l'ONU

Vie sociale et politique	
Droit au respect de la vie privée et familiale	art. 13 Cst., art. 8 CEDH, art. 17 Pacte civil de l'ONU
Droit au mariage et à la famille ou protection de la famille	art. 14 Cst., art. 8 et 12 CEDH, art. 23 Pacte civil de l'ONU, art. 10 Pacte social de l'ONU
Liberté de réunion	art. 22 Cst., art. 11 CEDH, art. 21 Pacte civil de l'ONU
Liberté d'association	art. 23 Cst., art. 11 CEDH, art. 22 Pacte civil de l'ONU, art. 8 Pacte social de l'ONU
Droit de pétition	art. 33 Cst.
Droits politiques	art. 34 Cst., art. 25 Pacte civil de l'ONU

Existence économique	
Garantie de la propriété	art. 26 Cst., art. 15 Pacte social de l'ONU
Liberté économique	art. 27 Cst.
Liberté syndicale et droit de grève	art. 28 Cst., art. 11 CEDH, art. 22 Pacte civil de l'ONU, art. 8 Pacte social de l'ONU
Interdiction de l'esclavage et du travail forcé	art. 4 CEDH, Art. 8 Pacte civil de l'ONU
Droit au travail	art. 6 Pacte social de l'ONU
Droit à des conditions de travail justes et favorables	art. 7 Pacte social de l'ONU
Droit d'obtenir de l'aide dans des situations de détresse	art. 12 Cst.
Droit à la sécurité sociale	art. 9 Pacte social de l'ONU
Droit à un niveau de vie suffisant (y compris pour la nourriture, les vêtements et le logement)	art. 11 Pacte social de l'ONU

Savoir	
Droit à un enseignement de base	art. 19 Cst., art. 13 et 14 Pacte social de l'ONU
Droit à l'éducation	art. 13 Pacte social de l'ONU
Liberté de la science	art. 20 Cst., art. 15 Pacte social de l'ONU
Droit de bénéficier du progrès scientifique	art. 15, al. 1, let. b, Pacte social de l'ONU
Protection de la propriété intellectuelle	art. 15, al. 1, let. c, Pacte social de l'ONU

Droits procéduraux	
Protection contre l'arbitraire	art. 9 Cst
Protection de la bonne foi	art. 9 Cst.
Droit à un procès équitable	art. 29, 29a et 30 Cst., art. 6 CEDH, art. 14 Pacte civil de l'ONU
Garanties procédurales en cas de privation de liberté	art. 31 Cst., art. 5 CEDH, art. 9, 10 et 11 Pacte civil de l'ONU
Garanties en procédure pénale	art. 32 Cst., art. 6 et 7 CEDH, art. 14 et 15 Pacte civil de l'ONU

Plusieurs conventions des Nations Unies sont également importantes pour la Suisse, notamment dans les domaines de la discrimination raciale, de l'interdiction de la torture ainsi que des droits des femmes, des enfants et des personnes en situation de handicap.

2.2.2 Les droits fondamentaux et les droits humains peuvent-ils être limités ?

Les États peuvent, à certaines conditions, limiter les droits fondamentaux et les droits humains. Concernant les droits fondamentaux, la Suisse a défini ces conditions à l'article 36 de la Constitution fédérale et les applique de façon similaire aux droits humains.

- En premier lieu, toute restriction doit être fondée sur une loi ou une ordonnance ; et si la limitation est d'une certaine gravité, elle doit être prévue dans une loi approuvée par le Parlement.
- En deuxième lieu, toute restriction doit reposer sur un juste motif. C'est le cas lorsqu'elle est justifiée par un intérêt public (comme le maintien de l'ordre public, la préservation de la santé publique ou la protection de l'environnement) ou par la préservation d'un droit fondamental d'autrui.
- En troisième lieu, toute restriction doit respecter le principe de proportionnalité. Pour être proportionnelle, une mesure doit être le moins sévère possible tout en conduisant à produire l'effet voulu. Elle doit aussi être proportionnée au but visé, et donc pouvoir être raisonnablement exigée.
- En quatrième et dernier lieu, tout droit fondamental possède un noyau intouchable qui ne peut en aucun cas être réduit.

Lorsqu'une limitation réunit ces quatre conditions, elle est licite. En l'absence d'une seule d'entre elles, elle est illicite et constitue par conséquent une violation des droits fondamentaux[47].

47 Pour des informations détaillées sur la limitation des droits fondamentaux, voir Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 9.

2.2.3 Que peut-on entreprendre en cas de violation d'un droit fondamental ou d'un droit humain ?

Dans tous les domaines de la vie, il peut arriver que l'État prenne des mesures qui portent atteinte à des droits fondamentaux ou à des droits humains. Pour que ces droits soient réellement protégés, les individus doivent disposer de moyens efficaces pour les faire respecter. Toute personne dont un droit fondamental ou un droit humain est lésé par la décision d'une autorité administrative ou par l'arrêt d'un tribunal peut porter son cas devant l'instance de recours, qui doit examiner si la décision ou l'arrêt en question est conforme aux droits fondamentaux et aux droits humains. Si cette instance constate une violation du droit en question, elle annule la décision ou l'arrêt. Si cela ne met pas fin à la violation de ce droit, la personne lésée a droit à une réparation[48].

2.2.4 Peut-on faire valoir tous les droits fondamentaux et les droits humains en justice ?

Les particuliers ne peuvent pas faire valoir tous leurs droits fondamentaux et leurs droits humains devant un tribunal. Le tableau ci-dessous[49] indique quels droits, selon la jurisprudence du Tribunal fédéral, il est possible de faire valoir en justice (ces droits sont dits « justiciables ») :

Sources du droit	Possibilité de faire valoir en justice
À l'échelle suisse	
Droits fondamentaux (art. 7 à 34 Cst.)	Oui
Buts sociaux (art. 41 Cst.)	Non
À l'échelle internationale	
Garanties de la CEDH	Oui
Garanties du Pacte civil de l'ONU	Oui
Garanties du Pacte social de l'ONU	Question controversée : selon le Tribunal fédéral, la plupart de ces garanties ne sont pas justiciables.
Garanties des autres conventions des droits humains de l'ONU	Le Tribunal fédéral décide au cas par cas si ces garanties sont justiciables.

48 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 8, ch. marg. 1 ss et 25 ss.

49 Ce tableau s'inspire de celui figurant dans : Egli, Egbuna-Joss, Ghielmini, Belser et Kaufmann, Droits fondamentaux des personnes âgées en Suisse, 2019, p. 21.

Il est en particulier impossible de faire valoir en justice les buts sociaux de la Constitution fédérale et la plupart des droits garantis par le Pacte social des Nations Unies (comme le droit à un logement ou à un niveau de vie adéquat). Le Tribunal fédéral estime en effet qu'il faut voir dans ces dispositions non pas des droits justiciables, mais un mandat octroyé au législateur pour réglementer des questions sociales.

2.2.5 Quelles sont les obligations de l'État ?

Les droits fondamentaux et les droits humains établissent surtout des obligations pour l'État. Ainsi, les parlements, tribunaux, gouvernements et administrations de la Confédération, des cantons et des communes doivent les respecter et contribuer à leur réalisation dans toutes leurs activités : adoption de lois, application de la justice et administration des collectivités publiques[50]. Cette obligation reste valable même lorsque l'État confie à des privés des tâches qui lui incombent (art. 35, al. 2, Cst.).

Par exemple, la fondation SWITCH gère pour le compte de l'Office fédéral de la communication le registre du domaine « .ch » ainsi que les domaines génériques de premier niveau (gTLD), tels que « .photo ». Étant donné que SWITCH accomplit une tâche publique pour le compte de l'État, elle est tenue, dans ce contexte, de respecter les droits fondamentaux et les droits humains[51].

Les droits fondamentaux et les droits humains confèrent à tout particulier trois types de droits subjectifs et imposent par conséquent trois genres d'obligations à l'État[52] :

En premier lieu, les individus peuvent exiger des autorités publiques qu'elles s'abstiennent, dans l'accomplissement de leurs tâches, de porter atteinte à leurs droits fondamentaux et à leurs droits humains. Ils ont en principe le

50 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 4, ch. marg. 39 ss et 42 ss.

51 ATF 138 I 289, consid. 2.3.

52 Au sujet de ces trois genres de droits et d'obligations, voir Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 4, ch. marg. 7 ss.

droit que l'État les « laisse en paix »[53]. L'État ne peut, par exemple, surveiller les activités d'un·e internaute que si des conditions très strictes sont réunies, pour élucider un crime notamment.

En deuxième lieu, dans certaines circonstances, les droits fondamentaux et les droits humains confèrent à l'État l'obligation de fournir certaines prestations. Pensons par exemple au droit à l'enseignement de base durant la pandémie de Covid-19 : les élèves ont alors suivi les cours à domicile. Si les enseignant·e·s ont eu recours à des outils didactiques en ligne, les écoles ont dû veiller à ce que chaque élève dispose des moyens techniques requis pour y avoir accès. Quand cela s'est avéré nécessaire, elles ont dû mettre à leur disposition des ordinateurs portables et des logiciels, fournissant ainsi une prestation publique (→ **cas pratique Enseignement scolaire en ligne 5.1**).

En troisième et dernier lieu, les droits fondamentaux et les droits humains créent aussi un droit à la protection, et donc une obligation de protéger : l'État doit faire en sorte que les droits des individus ne soient pas violés par des tiers (des particuliers ou des entreprises, par ex.). Ce devoir de protection est particulièrement important dans l'univers numérique, car ce sont souvent des particuliers et des entreprises privées qui portent atteinte aux droits des individus (→ **notions fondamentales point 2.2.7**).

2.2.6 Les personnes privées doivent-elles aussi respecter les droits fondamentaux et les droits humains ?

Quiconque s'intéresse à l'influence de la numérisation sur les droits fondamentaux et les droits humains s'apercevra rapidement que ce n'est souvent pas l'État qui viole ces droits, mais plutôt des particuliers ou des entreprises. Il peut par exemple y avoir violation du droit au respect de la vie privée lorsqu'un employeur surveille les courriels privés que ses employé·e·s envoient depuis le bureau ou lorsqu'une entreprise propose gratuitement une prestation sur une application, mais recueille en contrepartie les données des utilisateurs et utilisatrices pour leur envoyer ensuite des publicités personnalisées.

Les privés qui n'accomplissent pas de tâches publiques (comme c'est le cas du fournisseur de l'application ou de l'employeur dans les exemples ci-des-

53 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 4, ch. marg. 10.

sus) ne sont en principe pas directement tenus de respecter les droits fondamentaux et les droits humains[54]. L'article 35, alinéa 3 de la Constitution fédérale oblige certes les autorités à veiller à ce que les droits fondamentaux soient aussi une réalité dans les relations entre personnes privées, « dans la mesure où ils s'y prêtent », mais cette disposition n'a encore jamais été appliquée en justice[55]. Il faut donc établir s'il est malgré tout possible de protéger efficacement les particuliers contre les atteintes à leurs droits commises par d'autres privés.

Étant donné que les privés ne sont pas directement obligés de respecter les droits fondamentaux et les droits humains, un particulier ne peut pas recourir à un tribunal pour violation d'un droit fondamental ou d'un droit humain par un autre particulier ou une entreprise (comme le salarié en conflit avec son employeur). Malgré tout, ces droits exercent une influence sur les relations entre personnes privées, en raison du devoir de protection qu'ils imposent à l'État.

L'État doit en effet veiller à ce que les privés ne lèsent pas les droits fondamentaux et les droits humains d'autres privés[56]. Pour ce faire, il adopte par exemple des lois et des ordonnances qui réglementent les relations entre privés, comme les dispositions du code des obligations qui protègent les salarié·e·s et contraignent notamment l'employeur à respecter et à protéger leur droit à la vie privée. Dans un procès, des privés ne peuvent pas faire valoir directement les droits fondamentaux et les droits humains, mais peuvent faire référence à des lois qui en garantissent indirectement le respect aussi dans les relations entre personnes privées.

2.2.7 Quelles lois protègent les droits fondamentaux et les droits humains dans l'univers du numérique ?

Diverses lois protègent les particuliers contre les atteintes à leurs droits commises par d'autres privés dans le domaine numérique. Elles illustrent

54 Il existe quelques exceptions, comme le droit à un salaire égal pour un travail égal pour l'homme et la femme (art. 8, al. 3, Cst.).

55 Müller, Verwirklichung der Grundrechte, 2018, p. 58 ss.

56 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 4, ch. marg. 90.

bien la façon dont l'État concrétise l'obligation qui lui est faite de protéger les individus. Dans ce domaine, ce sont surtout les dispositions légales suivantes qui sont importantes en Suisse :

- *Protection de la personnalité :* les articles 28 et suivants du code civil interdisent toute atteinte à la personnalité commise par des tiers. Une atteinte à la personnalité est illicite lorsqu'aucun motif ne la justifie (comme un consentement ou un intérêt public). Il peut s'agir de propos diffamatoires ou de la publication de photos et d'informations privées. Dans l'univers du numérique, ces atteintes se propagent plus rapidement et atteignent un public plus important que dans le monde analogique (via les réseaux sociaux, par ex.). La victime peut demander au tribunal d'interdire ou de supprimer l'atteinte à sa personnalité et, suivant la situation, exiger des dommages-intérêts, une réparation et un droit de réponse[57].
- *Droit de la protection des données :* les lois fédérale et cantonales sur la protection des données garantissent notamment aux particuliers le droit au respect de leur vie privée lorsque des autorités publiques ou des entreprises traitent leurs données. La révision de la loi fédérale vient de se terminer et entrera probablement en vigueur en 2022[58]. Le traitement des données est en principe autorisé, à condition de respecter diverses consignes : les données personnelles ne doivent par exemple être traitées que dans le but qui est indiqué lors de leur collecte ou lorsqu'on peut logiquement le déduire des circonstances. Par ailleurs, elles doivent être correctes et protégées contre tout accès non autorisé (art. 4, 5 et 7 LPD ; art. 6 et 8 LPD rév.). Le traitement de données personnelles par des tiers ne doit pas porter une atteinte illicite à la personnalité de leur titulaire ; l'atteinte n'est toutefois pas illicite lorsque ces personnes ont donné leur consentement ou lorsqu'elle est justifiée par un intérêt privé ou public prépondérant (art. 12 et 13 LPD ; art. 30 et 31 LPD rév.). Enfin, toute victime peut demander qu'on mette fin au traitement de ses données, qu'on les corrige ou qu'on les détruise (art. 15 LPD ; art. 32 LPD rév.).

57 Büchler, Kommentar zu Art. 28 ff. ZGB, 2016.

58 Nous indiquons ici tant les dispositions encore valables de la LPD que celles de la version révisée (LPD rév.).

- *Droit du travail :* de nombreuses dispositions du droit du travail ont pour but de garantir le respect de la vie privée des salarié·e·s. Ainsi, l'article 328b du code des obligations interdit à l'employeur de collecter des données sur son personnel et de les analyser, à moins qu'elles ne présentent un lien étroit avec le travail, comme le nombre d'heures ou la qualité du travail effectué. Quant à l'article 26 de l'ordonnance 3 relative à la loi sur le travail, il interdit d'utiliser des systèmes de surveillance ou de contrôle uniquement pour surveiller le comportement des salarié·e·s à leur poste de travail. Si ces systèmes s'avèrent nécessaires pour d'autres raisons (comme la sécurité du personnel ou le contrôle des heures effectuées), ils doivent être utilisés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des membres du personnel.
- *Droit pénal :* certaines infractions ne peuvent être commises que dans l'univers numérique. Il s'agit par exemple de l'accès indu à un système informatique (art. 143bis CP) ou de l'utilisation frauduleuse d'un ordinateur (art. 147 CP). D'autres infractions ne s'inscrivent pas forcément dans un contexte numérique, mais peuvent aussi être commises à l'aide d'« outils » numériques : les menaces (art. 180 CP), la contrainte (art. 181 CP), la contrainte sexuelle (art. 189 CP) ou encore l'extorsion (art. 156 CP) sur les réseaux sociaux ou par courriel[59].
- *Loi contre la concurrence déloyale :* la loi fédérale contre la concurrence déloyale (LCD) vise à garantir une concurrence loyale, qui ne soit pas faussée. Divers actes relevant de la concurrence déloyale (art. 3 LCD) peuvent être commis plus facilement et diffusés à plus grande échelle grâce à la numérisation : dénigrer une entreprise ou les marchandises d'autrui (art. 3, al. 1er, let. a, LCD) ou envoyer de la publicité en masse en recourant à des outils de télécommunication (art. 3, al. 1er, let. o, LCD), par exemple. Il est notamment interdit, pour une entreprise, d'annoncer sur son site avoir déposé plainte pénale contre un concurrent avant que le ministère public ait admis ses accusations. Une telle annonce pourrait en effet semer le doute dans l'esprit de la clientèle quant au sérieux de l'entreprise incriminée[60].

59 Gyarmati, Cybercrime, 2019, p. 87.

60 Arrêt du Tribunal cantonal de Zoug, GVP 2013/1.2.5.1, 17.4.2013, consid. 4.2 s.

– *Droit d'auteur :* la loi sur le droit d'auteur (LDA) vise à protéger la propriété intellectuelle contre toute reproduction ou publication illégale. Elle a été revue dernièrement pour tenir compte des changements induits par la numérisation et en particulier l'éclosion de plateformes de piratage. Ainsi, les fournisseurs de services d'hébergement dont le modèle d'affaires génère un risque particulier de violation de la propriété intellectuelle sont désormais astreints à un devoir de surveillance. Ils doivent en conséquence prendre des dispositions pour qu'une œuvre téléchargée illégalement ne puisse pas être à nouveau téléchargée après avoir été supprimée (art. 39*d* LDA). Toutefois, les personnes qui font un usage privé d'une œuvre qu'elles ont téléchargée d'Internet peuvent continuer à le faire (art. 19 LDA), pour autant qu'elles ne mettent pas elles-mêmes des œuvres en ligne.

2.3 Influence de la numérisation sur les différents droits

Si elles peuvent contribuer à mieux protéger les droits fondamentaux et les droits humains, les technologies numériques sont aussi susceptibles de favoriser les violations ou les atteintes à ces droits. Dans les sections qui suivent, nous passerons dès lors en revue certains droits fondamentaux et droits humains particulièrement concernés afin de commenter l'impact que la numérisation a sur eux. Pour chacune des garanties étudiées, nous indiquons l'article de la Constitution fédérale qui s'y rapporte ainsi que les dispositions des conventions internationales dont la teneur est analogue. Nous avons classé ces droits en huit catégories : principes de base ; collecte de données et surveillance ; protection de l'intégrité physique et psychique ainsi que de la santé ; opinions, convictions et communication ; vie sociale et politique ; vie professionnelle et économie ; savoir ; enfin, démarches administratives et judiciaires.

2.3.1 Principes de base

A Dignité humaine[61]

Art. 7 Cst.

La dignité humaine doit être respectée et protégée.

La protection de la dignité humaine, première garantie figurant au catalogue des droits fondamentaux de la Constitution fédérale, est un principe que les autorités publiques doivent respecter en toute circonstance. Le Tribunal fédéral n'a pour l'instant pas déterminé de façon définitive la teneur précise de cette disposition. Pour l'essentiel, le respect de la dignité implique de reconnaître dans chaque personne un individu unique, ou différent, et de le traiter comme un être ayant une valeur intrinsèque.

La dignité humaine est bafouée lorsqu'un individu est traité comme un objet. Cette situation peut se produire lorsque des robots sont employés comme des aides-soignants (→ **notions fondamentales point 1.7** et **cas pratique Robots des soins 2.1**). On pourrait en effet considérer que ce recours à des robots transforme les soins en un simple travail d'entretien (similaire à ce qu'on ferait avec une machine), rabaisse la personne prise en charge au rang d'objet et bafoue ainsi sa dignité[62].

B Protection des enfants et des jeunes[63]

Art. 11 Cst.

Les enfants et les jeunes ont droit à une protection particulière de leur intégrité et à l'encouragement de leur développement.

Art. 41, al. 1, let. g, Cst. (but social) et art. 24 Pacte civil de l'ONU

En raison de la vulnérabilité des enfants et des jeunes, leur intégrité physique et psychique doit bénéficier d'une protection particulière. Dans ce domaine, la Convention des Nations Unies relative aux droits de l'enfant joue elle aussi un rôle important.

61 ATF 127 I 6, consid. 5b.

62 Kreis, Pflegeroboter, 2018, p. 224 s.

63 Biaggini, Kommentar zu Art. 11 BV, 2017, no 1 ss.

Le devoir d'octroyer une protection particulière aux enfants et aux jeunes ne signifie pas que les mineurs puissent faire valoir un droit précis en justice, mais oblige les pouvoirs publics à toujours tenir compte du bien de l'enfant lorsqu'ils concrétisent d'autres droits fondamentaux ou appliquent des lois se rapportant à d'autres thématiques. En outre, ce devoir contraint également l'État à édicter des lois et à prendre des mesures pour protéger les enfants et les jeunes.

Dans le domaine des technologies numériques, l'intégrité physique et psychique des enfants et des jeunes peut par exemple être mise en danger par le harcèlement sur les réseaux sociaux ou par la cyberdépendance. Ainsi, si une jeune fille est victime de cyberharcèlement, diverses dispositions du code pénal et du droit de la personnalité peuvent être appliquées pour la protéger (→ **cas pratique Cyberharcèlement 4.2**).

C Interdiction de la discrimination[64]

Art. 8, al. 2, Cst.

Nul ne doit subir de discrimination du fait notamment de son origine, de sa race, de son sexe, de son âge, de sa langue, de sa situation sociale, de son mode de vie, de ses convictions religieuses, philosophiques ou politiques ni du fait d'une déficience corporelle, mentale ou psychique.

Art. 8, al. 3 et 4 Cst. ; art. 14 CEDH ; art. 2, al. 2, Pacte social de l'ONU et art. 2, al. 1, Pacte civil de l'ONU

Le droit interdit tant la discrimination directe que la discrimination indirecte. Il y a discrimination directe lorsque l'État traite un individu différemment des autres, et donc le désavantage, du fait de l'une des caractéristiques énumérées ci-dessus, comme son âge, son genre ou son origine, et lorsqu'aucun motif objectif ne justifie cette inégalité de traitement. Si un logiciel servant à calculer le risque de récidive des personnes condamnées appliquait automatiquement un taux supérieur à toutes les personnes d'une certaine origine[65], nous serions en présence d'une discrimination directe.

64 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 36.

65 C'est le cas du logiciel COMPAS, qui a été utilisé aux États-Unis. À ce sujet, voir Zuiderveen Borgesius, Discrimination, 2018, p. 14 s.

La discrimination est dite indirecte lorsqu'une distinction est faite en fonction d'une caractéristique de prime abord « neutre » et non discriminatoire, mais qui aboutit tout de même à une inégalité de traitement pour une catégorie de personnes présentant l'une des caractéristiques protégées par la Constitution. Si, par exemple, le seul moyen d'obtenir une réduction des primes de caisse-maladie était de faire une demande par voie électronique, cette mesure ne constituerait pas, à première vue, une discrimination du fait de l'une de ces caractéristiques. Toutefois, en y regardant de plus près, on s'apercevrait que la proportion de personnes âgées dans l'incapacité de présenter une demande de réduction de primes par manque de compétences numériques serait bien plus élevée que celle des jeunes. En imposant cette exigence, l'administration discriminerait par conséquent les personnes aînées.

En principe, l'interdiction de la discrimination inscrite dans la Constitution fédérale ne s'applique qu'à l'action de l'État, car la Suisse ne s'est pas dotée d'une interdiction générale de discriminer qui s'appliquerait aux particuliers ou aux entreprises privées. Il existe néanmoins, dans certains domaines précis, comme le droit du travail, le droit du bail à loyer et le droit des assurances, des dispositions qui octroient une protection contre certains actes discriminatoires commis par des particuliers ou des entreprises privées[66].

Par ailleurs, les alinéas 3 et 4 de l'article 8 de la Constitution fédérale interdisent de discriminer deux catégories de personnes précises, les femmes et les personnes en situation de handicap, et exigent l'adoption de mesures afin d'éliminer les inégalités de traitement dont elles sont victimes. Ainsi, l'alinéa 3 consacre l'égalité en droit des hommes et des femmes dans toutes les situations de la vie et exige que le législateur adopte des lois afin de faire de cette égalité une réalité dans la loi et dans les faits, et cela dans les domaines de la famille, de la formation et du travail. Quant à l'alinéa 4, il demande que la Confédération légifère pour éliminer les inégalités auxquelles font face les personnes en situation de handicap.

Les technologies numériques peuvent dans une certaine mesure contribuer à instaurer l'égalité entre femmes et hommes et aussi à éliminer certaines inégalités subies par les personnes porteuses d'un handicap. Ainsi, les logiciels de vidéoconférence et de traitement à distance de documents partagés

66 Art. 271 CO, art. 336, al. 1, let. a, CO et art. 117, al. 2, OS.

permettent, pour différentes professions, de flexibiliser tant les lieux que les horaires de travail, ce qui peut aider à concilier vie familiale et vie professionnelle. Les expériences faites au printemps 2020 durant le confinement imposé par la pandémie de Covid-19 montrent cependant aussi que l'essor du travail à domicile peut rigidifier les rôles traditionnellement attribués à chaque genre[67].

Certaines techniques numériques, comme les logiciels de reconnaissance vocale ou les robots d'assistance, peuvent aider des personnes en situation de handicap à accomplir leurs tâches professionnelles ou à s'intégrer aux activités de la vie quotidienne. La rapidité des innovations technologiques et le remplacement des personnes par des robots risquent toutefois aussi de désavantager encore plus les porteurs et porteuses de handicap sur le marché du travail et de les exclure de ce marché[68].

2.3.2 Collecte de données et surveillance

A Droit au respect de la vie privée[69]

Art. 13, al. 1, Cst.

Toute personne a droit au respect de sa vie privée (…), de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications.

Art. 8 CEDH et art. 17 Pacte civil de l'ONU

La notion de vie privée, qui décrit le degré minimal d'intimité auquel chacun·e de nous a droit, constitue un champ dans lequel toute personne est libre de mener sa vie et d'entretenir des relations comme elle l'entend, sans que l'État n'intervienne d'aucune façon. Personne n'est obligé de communiquer aux autorités ou au public des informations d'ordre privé. Le droit au respect de la vie privée est lésé par exemple lorsqu'une conversation privée est enregistrée à l'insu des personnes qui y participent, peu importe que

67 Möhring, Naumann, Reifenscheid et al., Mannheimer Corona-Studie, 2020, p. 12 ss.

68 Conseil des États, postulat 16.4169, Environnement de travail inclusif, 2016.

69 Diggelmann, Kommentar zu Art. 13 BV, 2015 ; Breitenmoser et Schweizer, Kommentar zu Art. 13 BV, 2014.

l'échange ait lieu en public ou en privé. La surveillance de l'espace public au moyen d'un drone ou l'espionnage d'un immeuble portent eux aussi atteinte à la vie privée[70].

L'État doit respecter la vie privée de chaque individu, et cette protection s'étend au logement, à la correspondance et aux relations par la poste et les télécommunications (y compris les messages transmis par voie électronique, comme les courriels et les appels passés par téléphonie en ligne). Le droit à la vie privée peut être limité, lors d'enquêtes policières par exemple, mais la surveillance des communications (classiques ou électroniques) ou la perquisition du domicile ne sont admises que si elles remplissent de strictes conditions, définies par la loi.

L'État doit non seulement respecter le droit à la vie privée, mais aussi protéger les individus contre toute atteinte à leur vie privée commise par un particulier. Pour ce faire, il adopte par exemple des dispositions en matière de protection des données ou de droit du travail. Ces dispositions sont d'autant plus nécessaires qu'il est très facile, sur Internet, de diffuser rapidement des informations personnelles sans le consentement de l'individu concerné, informations qu'il est ensuite souvent difficile de supprimer.

B Droit à la protection des données[71]

Art. 13, al. 2, Cst.

Toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent.

Art. 8 CEDH et art. 17 Pacte civil de l'ONU

La Constitution fédérale consacre le droit à la protection des données et, comme corollaire, le droit à l'autodétermination informationnelle. En effet, contrairement à ce que laisse penser sa formulation, cet article n'instaure pas uniquement une protection contre le traitement abusif des données, mais octroie aussi à chaque personne le droit de décider en toute liberté si elle veut que ses données personnelles soient collectées, traitées, mémori-

70 Arrêt du Tribunal administratif fédéral A-2482/2007, 26.6.2007.

71 Diggelmann, Kommentar zu Art. 13 BV, 2015, no 32 ss ; Breitenmoser et Schweizer, Kommentar zu Art. 13 BV, 2014, no 70 ss.

sées et transmises. Ce droit protège les données dites à caractère personnel, soit les données qui se rapportent à une personne dont l'identité est connue, ou peut l'être, comme celles figurant dans son dossier médical ou des informations sur son apparence, sa situation économique, ses relations sociales ou ses opinions politiques.

Les gros volumes de données exploitées par des entreprises sont aussi collectés sur Internet et par les applications installées sur les smartphones. Ainsi, les gestionnaires de sites internet enregistrent les visites à l'aide de *cookies*, des fichiers qui permettent de déduire les intérêts, les habitudes et les traits de personnalité des internautes[72]. Les applications gratuites (traducteurs automatiques, jeux, outils de planification, etc.) collectent généralement elles aussi des données, ce dont les internautes ne sont souvent pas conscients.

Le droit à la protection des données s'applique au traitement des données tant par les pouvoirs publics que par des particuliers et des entreprises. Les lois fédérale et cantonales en la matière fixent plusieurs grandes lignes afin de protéger les données à caractère personnel : toute personne peut demander, tant à un service public qu'à une entreprise privée, si on y traite des données la concernant. Elle peut aussi exiger la suppression ou la rectification de ces données, en intentant une action en justice si nécessaire, et l'entité responsable du fichier doit effacer les données lorsque la loi l'y contraint ou lorsqu'aucun intérêt prépondérant public ou privé ne s'y oppose. Cette règle s'applique également aux données et aux images à caractère personnel publiées sur Internet (c'est ce que l'on appelle le droit à l'oubli, ou le droit au déréférencement). Toutefois, la suppression s'avère extrêmement difficile en pratique[73].

72 PFPDT, Explications concernant le webtracking, 2014.

73 Wermelinger, Kommentar zu Art. 15 DSG, 2015, no 9 s.

C Liberté de mouvement[74]

Art. 10, al. 2, Cst.

Tout être humain a droit (...) à la liberté de mouvement.

Art. 12, al. 1, Pacte civil de l'ONU

On entend par liberté de mouvement le droit de se déplacer à son gré sans être limité par l'État. Chaque personne est en principe libre de choisir les lieux où elle veut se rendre ou séjourner ainsi que ceux qu'elle préfère éviter.

Cette liberté de mouvement peut être limitée dans diverses situations, comme typiquement lors d'une détention, d'une interdiction de périmètre, de la fermeture de lieux publics (un parc, par ex.) ou d'une arrestation pour contrôle de police. Les technologies numériques peuvent jouer ici aussi un rôle : les instruments électroniques utilisés pour surveiller des personnes en détention (surveillance électronique) ou dépendantes (détecteurs de mouvements ou capteurs dans le matelas, par ex.)[75] peuvent porter atteinte à la liberté de mouvement également.

Les caméras de surveillance de l'espace public (rues, places), parfois combinées avec des logiciels de reconnaissance faciale, ne limitent certes pas directement la liberté de mouvement, car cet espace reste accessible. Néanmoins, elles peuvent la brider lorsque des personnes qui ne souhaitent pas être filmées ou enregistrées sont contraintes d'éviter les lieux publics où ces caméras sont installées (→ **cas pratique Vidéosurveillance étatique avec reconnaissance faciale dans l'espace public 3.5**)[76].

L'État n'est pas seulement tenu de respecter la liberté de mouvement dans son action, il doit aussi la protéger contre toute atteinte commise par des tiers, également lorsque des privés ont recours à des technologies numériques. Le droit du travail, par exemple, stipule à l'article 26 OLTr 3, que des

74 Schweizer, Kommentar zu Art. 10 BV, 2014, no 33 ss.

75 Egli, Egbuna-Joss, Ghielmini, Belser et Kaufmann, Droits fondamentaux des personnes âgées en Suisse, 2019, p. 47.

76 Schweizer, Kommentar zu Art. 10 BV, 2014, no 35.

systèmes de géolocalisation ou de surveillance vidéo ne peuvent être utilisés que s'ils ne portent pas atteinte à la liberté de mouvement des travailleurs et travailleuses (→ **cas pratique Surveillance au travail 1.3**)[77].

2.3.3 Protection de l'intégrité physique et psychique ainsi que de la santé

A Droit à la vie[78]

Art. 10, al. 1, Cst.

Tout être humain a droit à la vie.

Art. 2 CEDH et art. 6 Pacte civil de l'ONU

Le droit à la vie est le droit, pour les individus, d'une part de ne pas être tués par les autorités publiques et, d'autre part, de bénéficier de la protection de l'État si leur vie est menacée par autrui. En cas de violation du droit à la vie, les pouvoirs publics doivent mener une enquête et punir les coupables. Le droit à la vie peut être restreint dans des cas particuliers, par exemple lorsqu'une intervention de police absolument indispensable ne peut être réalisée d'une autre façon (« coup de feu mortel volontaire »)[79].

Le rapport entre le droit à la vie et les technologies numériques se manifeste notamment lorsqu'il faut déterminer s'il est licite, pour combattre le terrorisme, d'utiliser des drones pour tuer des individus précis[80].

77 SECO, Commentaire des ordonnances 3 et 4 Ltr, 2020, ch. marg. 326-1.

78 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 11.

79 Arrêt du Tribunal du canton des Grisons, SF 01 30, 28.2.2002, PKG 2002, p. 82 ss.

80 Rapporteur spécial des Nations Unies sur les droits de l'homme et la lutte contre le terrorisme, Rapport, 2017, ch. marg. 25 ss.

B Droit à l'intégrité physique et psychique[81]

> Art. 10, al. 2, Cst.
>
> Tout être humain a droit (…) à l'intégrité physique et psychique (…).

Le droit à l'intégrité physique interdit à l'État de porter une atteinte quelconque au corps d'un individu, indépendamment du fait qu'elle soit indolore ou douloureuse. Cet article comprend aussi le droit de disposer librement de son corps, et en particulier de décider de se soumettre ou non à des interventions médicales. Quant au droit à l'intégrité psychique, il protège la santé mentale et englobe le droit d'évaluer une situation sans subir l'influence de tiers, de prendre des décisions et d'agir comme on l'entend.

On peut imaginer plusieurs scénarios dans lesquels les technologies numériques peuvent porter atteinte à l'intégrité physique ou psychique : lorsqu'un robot de soins, par exemple, en raison d'une erreur de programmation, blesse une pensionnaire dans une maison de retraite (→ **cas pratique Robots des soins 2.1**). Quant à l'intégrité psychique, elle peut être mise en péril par le cyberharcèlement (→ **cas pratique Cyberharcèlement 4.2**) ou par le recours à des systèmes de surveillance permanente au lieu de travail ou dans l'espace public (→ **cas pratique Surveillance au travail 1.3**).

81 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 12, ch. marg. 18 ss et 25 ss.

C Interdiction de la torture et autres peines ou traitements inhumains ou dégradants[82]

Art. 10, al. 3, Cst.

La torture et tout autre traitement ou peine cruels, inhumains ou dégradants sont interdits.

Art. 3 CEDH et art. 7 Pacte civil de l'ONU

L'interdiction de la torture est un principe fondamental de l'État de droit qui ne peut, en aucun cas, être limité. Elle figure non seulement dans les sources de droit mentionnées ci-dessus, mais également dans la Convention des Nations Unies contre la torture[83].

La torture est interdite dans tous les cas, sans exception, que ce soit dans le cadre du travail de la police, dans des institutions telles que des établissements pénitentiaires, médico-sociaux ou psychiatriques ou encore des foyers pour personnes réfugiées. Par ailleurs, l'État doit protéger toutes les personnes contre des actes de torture commis par des personnes privées. Lorsque des accusations sont formulées, il doit mener l'enquête et punir les coupables, ce qu'il fait en appliquant principalement le droit pénal. Enfin, il ne peut refouler une personne de nationalité étrangère vers un pays dans lequel elle risque d'être torturée (interdiction du refoulement formulée à l'art. 25 Cst.).

Les technologies numériques peuvent contribuer à la violation de l'interdiction de la torture. Ainsi, des États peuvent surveiller des dissident·e·s politiques au moyen de ces technologies, pour ensuite les arrêter et les torturer[84]. L'interdiction de la torture s'applique aussi aux entreprises, car ce sont souvent des fournisseurs privés qui mettent au point ces technologies et les vendent aux États. Des entreprises suisses pourraient également être concernées par ce principe : l'État peut leur interdire d'exporter des sys-

82 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 13.

83 Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants.

84 Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Surveillance et droits de l'homme, 2019, ch. marg. 1 ; Point de contact britannique pour les Principes directeurs de l'OCDE à l'intention des entreprises multinationales, Privacy International et Gamma International UK LTD, déclaration finale, 2014.

tèmes de surveillance, en application de la législation sur le contrôle des biens, lorsqu'il est probable qu'ils seront utilisés pour réprimer des opposant·e·s[85]. Il existe toutefois aussi des logiciels qui aident les organisations de défense des droits humains à recueillir et à analyser des témoignages d'actes de torture et sont par conséquent susceptibles d'aider à élucider des cas[86].

D Droit à la santé[87]

Art. 41, al. 1, let. b, Cst. (but social)

La Confédération et les cantons s'engagent (…) à ce que toute personne bénéficie des soins nécessaires à sa santé.

Art. 12 Pacte social de l'ONU

Le droit à la santé est garanti par le Pacte social des Nations Unies et figure parmi les buts sociaux de la Constitution fédérale. On ne peut certes pas le faire valoir en justice, mais il confère à la Confédération et aux cantons l'obligation d'adopter des mesures pour le concrétiser. L'État doit en particulier veiller au bon fonctionnement du système de santé et garantir que toute la population puisse y avoir accès de manière égalitaire.

La numérisation peut contribuer à réaliser le droit à la santé : les outils de communication numériques constituent un canal supplémentaire d'accès à des conseils médicaux, tandis que l'intelligence artificielle et les mégadonnées facilitent par exemple la mise au point de nouveaux médicaments ou l'élaboration de plans de traitement personnalisés. Durant la pandémie de Covid-19, des applications contribuant à identifier les chaînes de contamination ont été conçues dans de nombreux pays, y compris en Suisse.

85 Ordonnance sur l'exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles.

86 Haut-Commissariat des Nations Unies aux droits de l'homme, Les droits humains dans une nouvelle ère, 2018.

87 Biaggini, Kommentar zu Art. 41 BV, 2017.

Toutefois, la collecte et le traitement de données médicales comportent un risque d'utilisation ou de publication abusive. On peut ainsi imaginer qu'une compagnie d'assurances puisse, sur la base de ces données, refuser de conclure une assurance complémentaire[88].

E Droit à la liberté personnelle[89]

> Art. 10, al. 2, Cst.
>
> Tout être humain a droit à la liberté personnelle (…).

Le droit à la liberté personnelle garantit à tout individu la possibilité de décider librement, sans ingérence de l'État, de tous les aspects qui concernent sa vie et sa personnalité. La liberté de choix qu'inclut la liberté personnelle n'instaure pas un droit absolu d'agir comme on l'entend en toute circonstance ; elle s'applique néanmoins aux aspects essentiels de la vie, tels que la façon de vivre sa sexualité, le désir d'avoir des enfants, les traitements médicaux et les décisions concernant la fin de vie.

La liberté personnelle garantit en principe aussi l'accès à la procréation médicalement assistée[90], bien que la Suisse interdise certains actes médicaux (don d'ovule et maternité de substitution, par ex.) ou les refuse aux couples homosexuels. La numérisation a favorisé la « mobilité de la reproduction », car les personnes souhaitant avoir recours à des méthodes interdites en Suisse peuvent plus facilement, sur Internet, avoir accès aux prestations proposées à l'étranger, échanger sur les réseaux sociaux et recevoir des conseils par vidéoconférence, ce qui renforce leur droit à la liberté personnelle.

88 Haut-Commissariat des Nations Unies aux droits de l'homme, Rôle des nouvelles technologies pour la réalisation des droits économiques, sociaux et culturels, 2020, ch. marg. 19 ss.

89 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 12.

90 ATF 119 Ia 460.

2.3.4 Opinions, convictions et communication

A Liberté de conscience et de croyance[91]

Art. 15 Cst.
La liberté de conscience et de croyance est garantie.
Art. 9 CEDH et art. 18 Pacte civil de l'ONU

La liberté de conscience et de croyance garantit le droit de choisir et de pratiquer librement toute religion, d'avoir sa propre conception du monde et d'adhérer ou non à une communauté. L'État doit protéger l'individu contre toute atteinte à sa liberté de religion par des personnes privées.

Des propos moqueurs, offensants ou discriminatoires à l'égard des fidèles d'une religion donnée circulent fréquemment sur les réseaux sociaux, en particulier dans leurs colonnes de commentaires. Ces propos peuvent, selon les circonstances, contrevenir à l'interdiction de l'atteinte à la liberté de croyance et des cultes (art. 261 CP) et de la discrimination raciale (art. 261bis CP) (→ **cas pratique Commentaires haineux sur Internet 4.1**).

Toutefois, la numérisation peut aussi faciliter la pratique de la religion. Ainsi, les vidéoconférences permettent maintenant d'assister à des services religieux ou d'entrer en contact avec un ou une responsable religieux, ce qui était impossible auparavant. En outre, grâce aux outils numériques, les fidèles souhaitant quitter une communauté peuvent obtenir plus facilement des informations et de l'aide pour le faire. Le confinement dû à la pandémie de Covid-19 a mis en exergue l'importance des modes de participation virtuelle (services religieux et pastoraux fournis par les Églises nationales sur des plateformes numériques).

91 Biaggini, Kommentar zu Art. 15 BV, 2017 ; Cavelti et Kley, Kommentar zu Art. 15 BV, 2014.

B Liberté d'opinion et d'information[92]

Art. 16 Cst.

La liberté d'opinion et la liberté d'information sont garanties.

Art. 10 CEDH et art. 19 Pacte civil de l'ONU

La liberté d'opinion désigne le droit de se forger sa propre opinion ainsi que de l'exprimer et de la diffuser sans entrave. On entend par opinion tout genre d'avis, d'appréciation, de conception et de sentiment ainsi que la diffusion d'informations et de nouvelles objectives. Les opinions peuvent aussi être critiques ou provocatrices.

L'État ne peut pas imposer une opinion déterminée aux individus ni exercer une censure préalable, mais il peut limiter cette liberté d'opinion pour protéger autrui. Par exemple, la personne injuriée sur un réseau social peut, en invoquant les dispositions du code civil protégeant la personnalité (art. 28 CC), exiger la suppression des propos insultants ou, dans certaines circonstances, déposer une plainte pénale pour injure (art. 177 CP) (→ **cas pratique Cyberharcèlement 4.2** et → **cas pratique Commentaires haineux sur Internet 4.1**).

La liberté d'information garantit le droit de se procurer, de recevoir et de transmettre des informations issues de sources accessibles au public. Elle est par conséquent indispensable à la libre formation de l'opinion. La publication par les pouvoirs publics d'informations importantes sur leurs sites internet contribue à renforcer la liberté de l'information (→ **cas pratique Des sites internet officiels accessibles 3.1**).

92 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 19 et 20.

C Liberté des médias[93]

Art. 17 Cst.

La liberté de la presse, de la radio et de la télévision, ainsi que des autres formes de diffusion de productions et d'informations ressortissant aux télécommunications publiques est garantie.

Art. 10 CEDH et art. 19 Pacte civil de l'ONU

Indissociable de la liberté d'opinion et d'information, la liberté des médias englobe tous les aspects de l'exercice du journalisme, comme les recherches, le choix des sujets et la diffusion du résultat de leurs travaux. On entend par communication médiatique, qui bénéficie de la liberté des médias, toute information transmise au public par un ou une journaliste, peu importe le support choisi pour le faire. Non seulement la presse écrite, la radio et la télévision, mais aussi tous les médias numériques, tels que des magazines en ligne, peuvent donc invoquer la liberté des médias.

La liberté des médias interdit la censure, protège les sources et garantit aux journalistes de pouvoir travailler sans ingérence externe. Comme la liberté d'opinion, elle peut aussi être limitée, par exemple pour protéger les droits de la personnalité de tiers.

D Liberté de la langue[94]

Art. 18 Cst.

La liberté de la langue est garantie.

Toute personne a le droit de s'exprimer dans la langue de son choix. Ce droit s'applique à toutes les langues et à tous les dialectes ainsi qu'aux langues des signes. Si cette liberté n'est pas limitée en privé, elle l'est dans les contacts avec les autorités : il faut alors s'exprimer dans une langue officielle.

93 Zeller et Kiener, Kommentar zu Art. 17 BV, 2015.

94 Biaggini, Kommentar zu Art. 18 BV, 2017.

S'ils peuvent favoriser la liberté de la langue, les logiciels de traduction peuvent aussi la limiter ; c'est le cas lorsqu'un programme de traduction ou de reconnaissance vocale ne reconnaît pas correctement certains dialectes ou certains accents.

E Liberté de l'art[95]

Art. 21 Cst.
La liberté de l'art est garantie.
Art. 15 Pacte social de l'ONU

La liberté de l'art garantit la création et la présentation d'œuvres dans toutes les formes d'expression artistique possibles : les artistes ont le droit de créer sans ingérence de l'État. Cette liberté peut toutefois être limitée pour protéger la personnalité d'autrui. Si la liberté de l'art ne permet pas d'exiger des pouvoirs publics qu'ils promeuvent des projets artistiques concrets, elle leur donne malgré tout l'obligation de poser un cadre favorable aux expressions artistiques.

Les œuvres créées à l'aide de techniques numériques bénéficient aussi de la liberté de l'art, que ces techniques soient utilisées pour créer une œuvre ou par la diffuser, la mémoriser ou la soumettre à une analyse scientifique. Les solutions numériques ne servent plus uniquement d'outil aux artistes, elles produisent elles-mêmes des œuvres de manière « indépendante ». Il existe ainsi des tableaux et des pièces de musique créés par le biais de l'intelligence artificielle[96], ce qui soulève de nouvelles questions juridiques concernant les droits d'auteur sur ces œuvres.

L'article 15, alinéa 1, lettre a du Pacte social de l'ONU consacre par ailleurs le droit de tout individu à prendre part à la vie culturelle. L'archivage numérique et la mise en ligne d'œuvres sur Internet facilitent considérablement la concrétisation de ce droit.

95 Biaggini, Kommentar zu Art. 21 BV, 2017.

96 SEFRI, Intelligence artificielle, 2019, p. 27.

2.3.5 Vie sociale et politique

A Droit au respect de la vie familiale[97]

Art. 13, al. 1, Cst.

Toute personne a droit au respect de sa vie (…) familiale (…).

Art. 41, al. 1, let. c Cst. (but social), art. 8 CEDH et art. 17 Pacte civil de l'ONU

Le droit au respect de la vie familiale garantit l'unité familiale et les contacts entre les membres de la famille. On entend par famille les couples mariés, les couples homosexuels, les couples en concubinage et les célibataires, ainsi que leurs enfants. Selon la situation et l'intimité des rapports, d'autres membres de la parenté tels que les grands-parents, peuvent aussi faire partie de la famille.

Les outils de communication numériques peuvent jouer un rôle en lien avec la limitation du droit au respect de la vie familiale en droit des étrangers, en particulier lorsqu'un membre de la famille est renvoyé du territoire suisse après une condamnation pénale. Dans ce cas en effet, le Tribunal fédéral estime que le parent expulsé peut en principe entretenir une relation familiale avec ses enfants mineurs vivant en Suisse en y faisant de brefs séjours ou par le biais de moyens de communication modernes, tels que les appels vidéo, et que son renvoi ne porte par conséquent pas atteinte à son droit à la vie de famille, ni à celui des enfants mineurs[98].

B Liberté de réunion[99]

Art. 22 Cst.

La liberté de réunion est garantie.

Art. 11 CEDH et art. 21 Pacte civil de l'ONU

La liberté de réunion comprend le droit d'organiser des réunions, d'y participer ou de s'en abstenir, et cela sans ingérence de la part de l'État. Les ou-

97 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 13, ch. marg. 22 ss.

98 ATF 144 I 91, consid. 5.1.

99 Biaggini, Kommentar zu Art. 22 BV, 2017.

tils de communication numériques peuvent être utilisés pour l'organisation et ont également le potentiel de mobiliser rapidement un grand nombre de personnes. Une réunion bénéficie de la protection accordée par la Constitution lorsque plusieurs personnes se rassemblent durant une période déterminée pour échanger ou exprimer leur opinion, durant une manifestation par exemple. La liberté de réunion ne s'étend pas aux rencontres virtuelles (telles que visioconférences ou forums de discussion[100]), mais ces dernières bénéficient, entre autres, de la liberté d'opinion. La liberté de réunion peut être limitée par exemple pour des raisons de sécurité ou, comme durant la pandémie de Covid-19, de santé publique.

C Droit de pétition[101]

> Art. 33 Cst.
>
> Toute personne a le droit, sans qu'elle en subisse de préjudice, d'adresser des pétitions aux autorités.

En vertu du droit de pétition, toute personne vivant en Suisse peut adresser ses préoccupations aux autorités, que ce soit sous forme de requêtes, de critiques et de propositions, et sur tous les sujets possibles. Ce droit est accordé tant aux particuliers qu'aux groupes d'individus. La numérisation intervient dans ce domaine notamment en permettant de récolter des signatures en ligne[102]. Si cette modalité simplifie les formalités et renforce ainsi le droit de pétition, elle peut aussi dissuader les personnes qui ne veulent pas que leur nom soit recueilli sur Internet dans ce contexte.

100 Errass, Kommentar zu Art. 22 BV, 2014, no 16.

101 Tschannen, Kommentar zu Art. 33 BV, 2015.

102 Conseil fédéral, Rapport CiviTech, 2020, p. 23 s.

D Droits politiques[103]

Art. 34 Cst.

Les droits politiques sont garantis.

La garantie des droits politiques protège la libre formation de l'opinion des citoyens et des citoyennes et l'expression fidèle et sûre de leur volonté.

Les droits politiques comprennent le droit de vote et le droit d'éligibilité, le droit de participer aux votations ainsi que le droit de lancer un référendum contre une loi votée par le Parlement et celui de déposer une initiative populaire. Les droits politiques garantissent aussi la libre formation de l'opinion et l'expression fidèle et sûre de la volonté des citoyens et des citoyennes. Les votant·e·s doivent pouvoir se déterminer sans ingérence externe : l'État a l'obligation de s'abstenir de les influencer dans la période qui précède les élections et les votations.

Les pouvoirs publics doivent aussi préserver la libre formation de l'opinion contre une emprise excessive exercée par des privés. Quant à ces derniers, ils ont fondamentalement le droit, dans l'exercice de leur liberté d'opinion, de s'exprimer sur les futures élections et votations. Internet, source d'informations et lieu d'échange, peut renforcer ce droit à la formation de la volonté, mais cette fonction n'est pas dépourvue de risques : des entreprises, des plateformes ou des partis politiques peuvent, grâce à des algorithmes, déterminer dans une large mesure quelles informations recevra un individu donné (bulle de filtres → **notions fondamentales point 1.2**) ou toucher des groupes de population précis à l'aide des techniques de microciblage (→ **notions fondamentales point 1.1**) pour influencer leurs opinions (→ **cas pratique Microciblage durant des campagnes politiques 3.4**)[104]. Lorsque des citoyens et citoyennes sont gravement induits en erreur sur des objets soumis à votation, les autorités fédérales, cantonales ou communales compétentes doivent intervenir et faire savoir, dans la mesure du possible, que les informations publiées par ces particuliers sont fausses. Elles peuvent aussi exceptionnellement être amenées à annuler la votation[105].

---

103 Biaggini, Kommentar zu Art. 34 BV, 2017.

104 PFPDT/Privatim, Guide concernant le traitement numérique de données personnelles dans le cadre d'élections et de votations en Suisse, 2019, p. 7.

105 ATF 135 I 292.

Ces dernières années, la Suisse a réalisé plusieurs essais de vote électronique, et cette modalité soulève deux questions : comment préserver le secret du vote lors de la transmission et de la conservation des bulletins de vote, et comment empêcher la manipulation des résultats des votations et des élections, que rendrait possible notamment le piratage de ces données[106] ? La Confédération envisage en outre d'introduire la récolte électronique des signatures, pour les initiatives populaires, par exemple[107].

2.3.6 Vie professionnelle et économie

A Garantie de la propriété[108]

Art. 26 Cst.

La propriété est garantie.

Art. 15, al. 1, let. c, Pacte social de l'ONU

La garantie de la propriété s'applique non seulement à la propriété matérielle et aux droits de jouissance des biens mobiliers et immobiliers, mais aussi à la propriété intellectuelle. Inscrite à l'article 15, alinéa 1, lettre c du Pacte social de l'ONU, cette dernière englobe des droits tels que les brevets et les droits d'auteur, mais pas les données à caractère personnel[109]. La garantie de la propriété protège avant tout les individus contre toute mainmise de l'État : si ce dernier s'empare de leur bien, il doit les indemniser. Elle impose aussi aux pouvoirs publics de protéger les personnes privées contre toute atteinte à leur droit de propriété par d'autres privés.

C'est surtout en matière de droits d'auteur que les technologies numériques touchent au droit de propriété. Elles permettent en effet de reproduire et de diffuser de façon presque illimitée des œuvres artistiques telles que livres, photographies, films et musique (notamment par le biais de services de flux) sans indemniser les titulaires du droit d'auteur ni demander leur consentement. En Suisse, la loi sur le droit d'auteur a été revue et adaptée à l'évolu-

106 Markić, Elektronische Stimmabgabe, 2019, p. 133 s.
107 Conseil fédéral, Rapport CiviTech, 2020, p. 22 s.
108 Biaggini, Kommentar zu Art. 26 BV, 2017.
109 Weber et Thouvenin, Dateneingentum, 2018.

tion de la technique ; ses nouvelles dispositions, en vigueur depuis le 1er avril 2020, prévoient notamment des mesures contre les plateformes de piratage (→ **notions fondamentales point 2.2.7**).

B Liberté économique[110]

> Art. 27 Cst.
>
> La liberté économique est garantie.

La liberté économique protège toute activité indépendante ou salariée visant à réaliser un bénéfice ou un gain. Elle garantit ainsi le libre choix de la profession, l'accès à une activité lucrative et le libre exercice de celle-ci. Elle comprend en particulier le droit de choisir librement, sans ingérence de l'État, les principales caractéristiques de toute activité commerciale, comme l'organisation ou la forme juridique d'une société ou encore le choix des collaborateurs et collaboratrices ainsi que des partenaires contractuels. En vertu de la liberté économique, l'État n'est pas autorisé à prendre des mesures faussant la concurrence entre les personnes privées ; par ailleurs, la législation sur les cartels protège ces derniers de toute restriction illicite à la concurrence commise par d'autres particuliers.

La liberté économique s'applique donc aussi à des modèles d'affaires décentralisés fondés sur Internet (économie des plateformes, économie de la chaîne de blocs, etc.). Toutefois, il est question actuellement de mieux réglementer les plateformes de mise en relation de services (comme les services de transport de personnes) et notamment de conférer aux prestataires le statut de salarié afin de mieux les protéger[111]. Si cette idée s'imposait, on limiterait la liberté économique pour renforcer la protection des travailleurs et travailleuses (→ **cas pratique Modèles d'affaires en ligne 6.2**).

110 Biaggini, Kommentar zu Art. 27 BV, 2017.

111 Abegg et Bernauer, Airbnb, Uber und Co., 2018, p. 84.

C Liberté d'association[112]

Art. 28 Cst.

Les travailleurs, les employeurs et leurs organisations ont le droit de se syndiquer pour la défense de leurs intérêts, de créer des associations et d'y adhérer ou non.

Art. 11 CEDH, art. 8 Pacte social de l'ONU et art. 22 Pacte civil de l'ONU

La liberté d'association comprend le droit de tous les travailleurs et travailleuses, des employeurs et de leurs organisations (syndicats et organisations patronales) de s'unir et d'agir pour défendre ensemble leurs intérêts, sans ingérence de l'État. Elle garantit aussi, outre le droit de grève, le droit à la négociation collective et le droit de réglementer les conditions de travail en concluant des conventions collectives de travail.

Les personnes dont l'activité professionnelle est gérée par des plateformes numériques ou qui travaillent surtout à domicile ont moins de possibilités d'échanger avec d'autres travailleurs et travailleuses et avec des organisations syndicales, ce qui peut restreindre leur liberté d'association[113].

D Travail exercé dans des conditions équitables[114]

Art. 41, al. 1, let. d, Cst. (but social)

La Confédération et les cantons s'engagent (…) à ce que toute personne capable de travailler puisse assurer son entretien par un travail qu'elle exerce dans des conditions équitables.

Art. 6 et 7 Pacte social de l'ONU

Le Pacte social des Nations Unies garantit le droit au travail (art. 6) et le droit de jouir de conditions de travail appropriées (art. 7). Le but social de la Constitution fédérale – toute personne capable de travailler doit pouvoir assurer son entretien par un travail qu'elle exerce dans des conditions équitables – va dans le même sens. Ces dispositions n'octroient pas aux individus vivant en Suisse un droit subjectif à un emploi ou à des conditions de tra-

112 Biaggini, Kommentar zu Art. 28 BV, 2017.

113 Conseil fédéral, numérisation et conditions de travail, 2017, p. 77 s. ; USS, Dossier no 125 Numérisation, 2017, p. 25 s.

114 Biaggini, Kommentar zu Art. 41 BV, 2017.

vail déterminées qu'ils pourraient faire valoir en justice. Elles donnent néanmoins aux autorités cantonales et fédérales le mandat d'agir pour que le plus grand nombre possible de personnes actives aient un emploi (en prenant par exemple des mesures favorisant les demandeurs et demandeuses d'emploi) et pour que les conditions prévalant sur le marché du travail soient équitables (en adoptant par exemple des dispositions ad hoc dans la loi sur le travail ou en étendant le champ d'application des conventions collectives de travail).

La rapidité des évolutions technologiques exerce divers effets sur les travailleurs et travailleuses, leurs droits et leur protection. Il s'avère par exemple que ce sont en particulier les travailleurs et travailleuses âgés qui ne disposent pas des connaissances informatiques exigées sur le marché du travail, de sorte que l'organisation de cours dans ce domaine constitue une mesure particulièrement importante[115].

Certaines technologies numériques (comme les caméras, la géolocalisation ou d'autres logiciels) peuvent être utilisées pour surveiller le personnel. D'autres remplacent l'être humain dans l'accomplissement d'une partie de ses tâches. La Poste a par exemple commencé à réaliser des essais pour confier la distribution du courrier à des robots[116]. La numérisation aboutit aussi souvent à une augmentation du rythme de travail et du contrôle des opérations effectuées par chaque travailleur ou travailleuse, ce qui peut générer davantage de stress et, par conséquent, des problèmes de santé. Elle entraîne par ailleurs la réorganisation de diverses tâches qu'accomplissaient auparavant des salarié·e·s. Ainsi, les personnes qui offrent leurs services par le biais de plateformes numériques ne sont généralement pas considérées comme salariées, mais comme indépendantes. Elles ne bénéficient donc pas des garanties habituelles du droit du travail (délais de congé, poursuite du paiement du salaire en cas de maladie, durée maximale du travail, etc.) (→ **cas pratique Modèles d'affaires en ligne 6.2**). D'autres activités sont entièrement externalisées, selon le modèle de *crowdsourcing* ou production participative, et sont souvent bénévoles (c'est le cas par exemple des contributions dans Wikipédia).

115 Egger, Dreher et Partner, Arbeitsmarktliche Massnahmen, 2019, p. 11 et 66.

116 Tagesanzeiger, Lieferroboter, 2019.

Cependant, les technologies numériques peuvent aussi être utilisées pour garantir le respect de certaines normes minimales du droit du travail. Le Conseil fédéral entend par exemple étudier la façon d'appliquer la technologie de la chaîne de blocs (→ **notions fondamentales point 1.8**) pour faciliter la traçabilité de la filière de l'or et contribuer de la sorte au respect des normes du travail dans le secteur minier[117].

E Droit à la sécurité sociale[118]

Art. 41, al. 1, let. a, Cst. (but social)

La Confédération et les cantons s'engagent (...) à ce que toute personne bénéficie de la sécurité sociale.

Art. 9 Pacte social de l'ONU

Le droit à la sécurité sociale est garanti par le Pacte social des Nations Unies et figure parmi les buts sociaux de la Constitution fédérale. Si on ne peut pas le faire valoir en justice en Suisse, il donne néanmoins pour mission à la Confédération et aux cantons d'œuvrer afin que toute personne bénéficie de la sécurité sociale. En Suisse, ce sont surtout les assurances sociales qui contribuent à réaliser ce but : la prévoyance vieillesse, survivants et invalidité (avec ses trois piliers), l'assurance-chômage, l'assurance-maternité, l'assurance-maladie et accidents ainsi que, à l'échelon cantonal, l'aide sociale et les allocations familiales.

Dans le domaine de la sécurité sociale, on peut utiliser des logiciels pour examiner le droit d'un·e assuré·e à bénéficier d'une mesure, calculer le montant d'une prestation ou détecter des demandes abusives[119]. En l'occurrence, il faut se demander comment paramétrer les algorithmes utilisés (→ **notions fondamentales point 1.2**) pour que les décisions prises respectent l'égalité de droit, l'interdiction de la discrimination et le droit à la sécurité sociale.

117 Conseil fédéral, Commerce de l'or produit en violation des droits humains, 2018, p. 12.

118 Biaggini, Kommentar zu Art. 41 BV, 2017.

119 Rapporteur spécial des Nations Unies sur les droits de l'homme et l'extrême pauvreté, État-providence numérique, 2019.

2.3.7 Savoir

A Droit à un enseignement de base[120]

Art. 19 Cst. Le droit à un enseignement de base suffisant et gratuit est garanti.
Art. 13 et 14 Pacte social de l'ONU

Chaque enfant vivant en Suisse a droit à un enseignement de base suffisant et gratuit, et donc à une prestation concrète de l'État. Il s'agit là d'un droit que l'on peut faire valoir en justice. L'enseignement de base est considéré comme suffisant lorsqu'il prépare l'enfant à mener une vie indépendante au sein de la société d'aujourd'hui.

Ce droit à un enseignement de base peut être limité, par exemple lorsque l'élève est exclu·e de son établissement scolaire pendant un certain temps pour des raisons disciplinaires ou que les cours sont donnés à distance durant une période donnée, comme cela s'est produit lorsque les écoles ont été fermées durant la pandémie de Covid-19. Dans des situations de ce genre, le matériel didactique en ligne ou les visioconférences permettent dans une certaine mesure de continuer à dispenser un enseignement. Il y a violation du droit à un enseignement de base lorsque l'enseignement est si limité que l'égalité des chances entre élèves n'est plus garantie ou qu'il n'est plus possible d'assurer la transmission de contenus jugés indispensables pour notre société (→ **cas pratique Enseignement scolaire en ligne 5.1**).

120 Biaggini, Kommentar zu Art. 19 BV, 2017.

B Droit à l'éducation[121]

Art. 41, al. 1, let. f, Cst. (but social)

La Confédération et les cantons s'engagent à ce que (...) les enfants et les jeunes ainsi que les personnes en âge de travailler puissent bénéficier d'une formation initiale et d'une formation continue correspondant à leurs aptitudes.

Art. 13 Pacte social de l'ONU

L'article 13 du Pacte social de l'ONU consacre le droit à l'éducation, qui comprend tant la scolarisation des enfants que la formation des adultes. Sa teneur est similaire au but social figurant à l'article 41, alinéa 1er, lettre f de la Constitution fédérale qui donne à la Confédération et aux cantons le mandat de veiller à ce que les enfants et les jeunes ainsi que les personnes en âge de travailler puissent bénéficier d'une formation initiale et d'une formation continue adaptées à leurs capacités.

Contrairement au droit à un enseignement de base, le droit à l'éducation ne peut faire l'objet d'une action en justice en Suisse, car sa définition est, de l'avis du Tribunal fédéral, trop imprécise pour que l'on puisse en déduire des droits concrets[122]. Toutefois, l'État a l'obligation d'adopter des lois et de prendre d'autres mesures pour que tous les enfants, adolescents et adultes puissent bénéficier d'une formation de base et d'une formation continue suffisantes.

Les technologies numériques présentent un vaste potentiel en matière de droit à l'éducation, puisqu'elles donnent aux apprenant·e·s et aux enseignant·e·s un accès pratiquement illimité à des outils didactiques tels que livres numériques, vidéos et didacticiels interactifs. Elles sont en outre à la base des MOOC[123], des formations à distance, et donc accessibles de n'importe où, souvent gratuites. La numérisation peut cependant aussi menacer l'égalité des chances. Les programmes d'apprentissage numériques sont en effet réservés aux personnes qui disposent d'une connexion internet ainsi que du matériel, des logiciels et des connaissances nécessaires. Dès lors, les

121 Kägi-Diener, Kommentar zu Art. 19 BV, 2014, no 4.

122 ATF 126 I 240, consid. 2 s.

123 Les MOOC (Massive Open Online Courses), aussi appelés FLOT (pour formation en ligne ouverte à tous), sont des cours que toute personne intéressée peut suivre, sans restriction d'accès.

personnes qui n'y ont pas accès, pour des raisons d'ordre financier ou autre, peuvent être désavantagées : c'est ce que l'on appelle la fracture numérique (→ **cas pratique Enseignement scolaire en ligne 5.1**)[124].

C Liberté de la science[125]

Art. 20 Cst.

La liberté de l'enseignement et de la recherche scientifiques est garantie.

Art. 15, al. 1, let. b, Pacte social de l'ONU

L'enseignement et la recherche scientifiques ainsi que la publication des résultats de la recherche bénéficient de la liberté de la science, une liberté qui s'étend également à toute recherche sur les technologies numériques. Cette disposition garantit le droit de se livrer à des recherches sans ingérence de l'État et de prendre connaissance du résultat des recherches menées par d'autres scientifiques. Elle interdit aussi la censure systématique du contenu des articles scientifiques. Si elle n'octroie pas aux chercheurs et chercheuses un droit à des subventions qu'ils pourraient faire valoir directement en justice, la liberté de la science donne néanmoins à l'État le mandat de promouvoir la science en mettant les infrastructures nécessaires à leur disposition. Cette liberté peut par exemple être restreinte par le budget consacré à la science ou par les axes de recherche qui sont définis dans les programmes de subventions.

Par ailleurs, l'article 15, alinéa 1er, lettre b du Pacte social de l'ONU garantit à chaque individu le droit de bénéficier des avancées scientifiques et de leurs applications. Ce droit ne peut certes pas faire l'objet d'une action en justice, mais l'État a le devoir de veiller à la conservation et à la diffusion des résultats de la recherche. En outre, toute personne doit pouvoir en bénéficier

124 Rapporteur spécial des Nations Unies sur le droit à l'éducation, Droit à l'éducation à l'ère numérique, 2016, ch. marg. 26 ss et 31 ss.

125 Kiener, Kälin et Wyttenbach, Grundrechte, 2018, chap. 24.

dans la même mesure. La promotion des publications en libre accès par les pouvoirs publics constitue un pas dans cette direction (→ **cas pratique Publication d'une étude scientifique 5.2**)[126].

2.3.8 Démarches administratives et judiciaires

A Protection de la bonne foi[127]

Art. 9 Cst.

Toute personne a le droit d'être traitée par les organes de l'État (…) conformément aux règles de la bonne foi.

Le droit d'être traité conformément aux règles de la bonne foi signifie que les individus peuvent faire confiance aux informations fournies par les autorités et agir en conséquence. Si une personne a agi en se fiant à un renseignement donné par une autorité publique et que cette information se révèle fausse, elle ne doit pas subir les conséquences de cette erreur, notamment pas sur le plan financier (protection de la confiance). Le contexte de la numérisation amène donc à se demander, par exemple, si des *tweets* publiés par des membres d'une autorité publique constituent une déclaration juridiquement contraignante, à laquelle les individus peuvent se fier[128].

B Droit à un procès équitable[129]

Art. 29, 29a, 30 et 32 Cst.

Toute personne a droit à un procès équitable.

Art. 6 et 7 CEDH et art. 14 et 15 Pacte civil de l'ONU

Le droit à un procès équitable comprend de nombreuses facettes régies par diverses dispositions de la Constitution fédérale. Ainsi, toute personne a droit, dans une procédure judiciaire ou administrative, à ce que sa cause

126 Comité des droits économiques, sociaux et culturels des Nations Unies, observation générale no 25, 2020, ch. marg. 4 ss et 45 ss.

127 Biaggini, Kommentar zu Art. 9 BV, 2017, no 13 ss.

128 Langer, Staatliche Nutzung von Social Media-Plattformen, p. 954 ss.

129 Biaggini, Kommentar zu Art. 29, 29a, 30 und 32 BV, 2017.

soit traitée équitablement et jugée dans un délai raisonnable. Elle a aussi le droit de s'exprimer durant la procédure (droit d'être entendu) et, si elle ne dispose pas de ressources suffisantes, le droit de demander que l'État prenne en charge les frais de procédure et les frais d'avocat (art. 29 Cst.). Par ailleurs, elle a droit à ce que sa cause soit jugée non seulement par une autorité administrative, mais aussi par un tribunal (art. 29a Cst.), qui doit être indépendant et impartial (art. 30 Cst.).

Pour les procédures pénales, la Constitution fédérale formule des garanties supplémentaires à son article 32 : toute personne est ainsi présumée innocente tant qu'elle n'a pas été condamnée ; les prévenu·e·s doivent par ailleurs être informés immédiatement des accusations dont ils font l'objet et avoir la possibilité de se défendre.

L'État emploie divers types de logiciels en procédure pénale. En Suisse, la police par exemple utilise plusieurs programmes qui, en recourant à l'intelligence artificielle, prédisent les délits par zone, ce qui lui permet de planifier ses patrouilles en conséquence (police prédictive)[130]. Il existe aussi des logiciels conçus pour déterminer le montant des peines, mais ils ne sont pas utilisés en Suisse[131]. Ces logiciels soulèvent plusieurs questions s'agissant du droit à un procès équitable : comment respecter par exemple le droit d'être entendu lorsque des aspects essentiels de la peine ou de la libération conditionnelle sont calculés par un logiciel dont l'algorithme est incompréhensible pour la personne concernée ? Et comment vérifie-t-on que le logiciel est programmé de façon indépendante et impartiale (→ **cas pratique Automatisation des décisions administratives 3.2** et **cas pratique Automatisation d'évaluations de risque 3.3**) ?

130 Camavdic, Predictive Policing in der Schweiz, 2019, ch. marg. 4 ss.

131 Vegh, Künstliche Intelligenz in der Strafzumessung, 2019, p. 363.

C Garanties procédurales en cas de privation de liberté[132]

Art. 31 Cst.

Nul ne peut être privé de sa liberté si ce n'est dans les cas prévus par la loi et selon les formes qu'elle prescrit.

Art. 5 CEDH, art. 9, 10 et 11 Pacte civil de l'ONU

La Constitution fédérale prévoit plusieurs garanties en cas de privation de liberté. Une personne ne peut par exemple être privée de sa liberté que dans les cas définis par la loi et doit être aussitôt informée, dans une langue qu'elle comprend, de ses droits et des raisons de cette privation ; elle doit également pouvoir en informer ses proches. En outre, un tribunal doit régulièrement vérifier si la privation de liberté est conforme à la loi.

On parle de privation de liberté lorsqu'une personne est retenue quelque part contre son gré durant un certain temps. Cette notion ne recouvre pas seulement la peine de prison, la détention ou le placement à des fins d'assistance dans un établissement médical, mais aussi de nouvelles modalités de privation de liberté rendues possibles par la numérisation, comme l'assignation à domicile au moyen d'un bracelet électronique (surveillance électronique)[133].

132 Biaggini, Kommentar zu Art. 31 BV, 2017.

133 Wohlers, Kommentar zu Art. 79b StGB, 2020, no 1 ss.

Deuxième partie

Présentation de cas pratiques

Nous montrons dans cette partie, à l'aide d'exemples concrets, en quoi les technologies numériques peuvent consolider les droits fondamentaux et les droits humains ou les compromettre. Pour chaque problématique que la numérisation a générée ou contribué à générer, nous présentons un cas fictif illustrant le propos. Nous abordons ensuite les libertés et droits fondamentaux en jeu ainsi que les questions juridiques soulevées, pour conclure par une brève présentation des possibilités d'action. Des indications supplémentaires, notamment sur la pratique des tribunaux, complètent ces cas[134].

Les exemples de cas ont été choisis de manière à aborder une palette aussi large que possible de situations de la vie quotidienne : travail, santé, démarches administratives, judiciaires et politiques, utilisation d'Internet, éducation et recherche ainsi qu'économie. Nous y traitons tant l'action des pouvoirs publics que celle des particuliers ou des entreprises, et montrons en quoi cette action soulève des questions liées aux droits fondamentaux et aux droits humains. Les faits exposés sont tous fictifs, mais ont été élaborés sur la base d'entretiens menés avec des professionnel·le·s ; certains d'entre eux s'inspirent d'arrêts rendus par le Tribunal fédéral ou de cas survenus à l'étranger.

Nous ne nous livrons pas à une analyse exhaustive des conditions à remplir pour limiter les droits fondamentaux et les droits humains concernés, mais nous nous concentrons sur les aspects qui s'avèrent décisifs dans le contexte de chaque cas. Afin d'en rendre la substance bien compréhensible, nous avons en outre simplifié les faits lorsque cela s'est avéré nécessaire, ce qui fait de cet ouvrage un guide pratique, et pas juridique.

---

134 La structure de présentation des cas reprend celle des publications suivantes : Akkaya, Grund- und Menschenrechte in der Sozialhilfe, 2015 ; Akkaya, Belser, Egbuna-Joss et Jung-Blattmann, Grund- und Menschenrechte von Menschen mit Behinderungen, 2016 ; Egli, Egbuna-Joss, Ghielmini, Belser et Kaufmann, Droits fondamentaux des personnes âgées en Suisse – un guide pratique, 2019.

1 Travail

1.1 Un algorithme sélectionne les dossiers de candidature

Madame A., qui a répondu à une offre d'emploi, reçoit une réponse négative sans avoir été invitée à un entretien. Elle apprend par la suite que l'entreprise en question a eu recours lors de la présélection des dossiers à un logiciel qui, sur la centaine de postulations reçues, n'a retenu que dix candidat·e·s à convier à un entretien. Étant donné que ce logiciel a été développé par un tiers, personne au sein du service des ressources humaines ne peut expliquer à Madame A. pour quelle raison elle n'a pas été invitée à un entretien.

Droits en jeu

– Interdiction de la discrimination

Question juridique

L'utilisation d'un logiciel pour réaliser une présélection des candidat·e·s à un poste peut-elle constituer une violation de l'interdiction de la discrimination ?

Analyse juridique

Le logiciel utilisé se fonde sur un algorithme qui recherche certaines caractéristiques précises dans les jeux de données qu'il analyse. Concrètement, pour évaluer les dossiers de candidature, il se fonde sur les caractéristiques des profils de candidat·e·s que l'entreprise en question a embauchés durant les dernières années. L'algorithme a déterminé lui-même ces caractéristiques de manière autonome, c'est-à-dire sans intervention humaine, en se fondant sur un jeu de données d'entraînement tiré des dossiers de candidature précédents (→ **notions fondamentales point 1.3**).

Pour déterminer s'il y a eu violation de l'interdiction de discriminer, il faut tout d'abord savoir si Madame A. a postulé auprès d'une entreprise privée

ou d'un organisme public. L'État est, en tant qu'employeur, tenu de respecter la Constitution fédérale et l'interdiction qui y figure. Il n'en va pas de même des employeurs privés, auxquels l'interdiction de discriminer inscrite dans la Constitution ne s'applique pas directement, mais qui sont soumis aux dispositions du droit du travail et du code des obligations (→ **notions fondamentales point 2.2.7**). Or, l'article 328 du code des obligations oblige à respecter la personnalité des travailleurs et travailleuses et à prendre des mesures pour la protéger, ce qui signifie notamment qu'il est interdit, également aux employeurs privés, de discriminer leurs employé·e·s. Tant pour les employeurs publics que pour les employeurs privés, cette interdiction de la discrimination n'est pas seulement valable une fois le contrat de travail conclu, mais déjà durant le processus de recrutement[135].

Le recours à un algorithme pour sélectionner les meilleurs candidats et candidates constituerait une violation de l'interdiction de discriminer si l'algorithme se fondait sur des critères tels que l'âge, le genre ou l'origine des candidat·e·s, autant de caractéristiques qu'il est illicite de prendre en compte. Toutefois, même s'il se fonde sur des caractéristiques objectives et non discriminatoires, un algorithme peut, dans la pratique, désavantager des personnes en raison de leur âge ou de leur genre, par exemple : un algorithme qui filtre les dossiers en fonction de critères tirés des profils des personnes engagées durant les dernières années désavantagera les candidatures féminines si l'entreprise a embauché davantage d'hommes que de femmes durant cette période[136]. C'est ce qui s'est passé dans notre cas pratique.

Pour conclure à une violation de l'interdiction de discriminer, il faudrait aussi qu'il n'y ait pas de motif particulier justifiant le fait d'exclure certaines personnes ou d'en sélectionner d'autres. Il est ainsi permis d'écarter les candidat·e·s ne présentant pas une caractéristique absolument indispensable pour occuper le poste à pourvoir. Les Églises peuvent par exemple exiger de leurs employé·e·s l'appartenance à une religion déterminée.

Conclusions et recommandations

S'il s'avère que la candidature de Mme A. n'a pas été retenue en raison de son genre, cette dernière ne peut certes pas revendiquer le droit d'être en-

135 Pellascio, Kommentar zu Art. 328 OR, 2016, no 9 et 16.

136 Wildhaber, Robotik am Arbeitsplatz, 2017, p. 215.

gagée, mais elle peut prétendre au versement d'une indemnité (art. 5, al. 2, LEg) : il lui faudra pour cela engager une procédure administrative si l'employeur est une institution publique ou une procédure de droit civil s'il s'agit d'un employeur privé.

Ses chances d'aboutir sont toutefois minces. Il est quasiment impossible, pour qui que ce soit, de déterminer sur la base d'une seule réponse négative si l'algorithme utilisé présente un élément discriminatoire. Dans le cas qui nous occupe ici, même les employé·e·s des ressources humaines n'étaient pas capables de déterminer les critères que l'algorithme a appliqués pour évaluer les dossiers de candidature. En fin de compte, il n'est donc pas possible de savoir sur la base de quelles caractéristiques les décisions ont été prises, et si l'éventuelle inégalité de traitement était justifiée ou non.

Comme nous l'avons expliqué ci-dessus, il y a ou non discrimination en fonction des caractéristiques que le logiciel prend en compte pour trier les candidatures. Il est par conséquent décisif de déterminer quels critères l'algorithme peut retenir pour effectuer sa sélection. Pour éviter toute discrimination directe ou indirecte, il est important que les personnes qui programment le logiciel vérifient s'il contient des caractéristiques discriminatoires telles que le genre et réalisent des tests pour voir comment le logiciel y réagit. Elles doivent aussi veiller à ce que le jeu de données d'entraînement de l'algorithme couvre une gamme aussi variée que possible de candidatures retenues par le passé. De plus, l'algorithme ne doit pas exclure des dossiers en se fondant sur des caractéristiques qui n'ont aucun lien avec l'aptitude à occuper le poste en question. Les concepteurs et conceptrices doivent en outre indiquer de manière transparente les caractéristiques avec lesquelles ils ont programmé l'algorithme[137]. Enfin, une personne – et pas un logiciel – devrait vérifier que les résultats fournis par l'algorithme sont plausibles et respectent les droits fondamentaux et les droits humains.

Informations supplémentaires

En Suisse, des services du personnel recourent à des logiciels pour évaluer des dossiers de candidature[138]. L'exemple présenté ci-dessus s'inspire toutefois d'un cas survenu à l'étranger. L'entreprise Amazon avait testé durant

137 Söbbing, Künstliche Intelligenz im HR-Recruiting-Prozess, 2018, p. 65.

138 Glatthaar, Robot Recruiting, 2020, p. 43 ss, Schafheitle et Weibel, HR Tech Survey, 2020.

un certain temps un logiciel de recrutement, avant de finir par y renoncer. L'algorithme en question avait été développé sur la base de données des membres du personnel, au moyen de l'apprentissage automatique. Comme le personnel d'Amazon comptait surtout des hommes, l'algorithme en avait conclu que l'entreprise préférait engager des hommes. Il avait identifié dans le fait d'être de genre masculin un critère d'embauche décisif et a par conséquent privilégié les candidatures masculines[139].

139 Dastin, AI recruiting tool, 2018.

1.2 Postulations et réseaux sociaux

Monsieur B., qui a postulé auprès d'une entreprise, reçoit une réponse négative. Durant la procédure de sélection, une employée du service du personnel a fait une recherche sur quelques réseaux sociaux, par pure curiosité, et a trouvé des photos de lui durant ses dernières vacances, en train de faire la fête de manière plutôt délurée.

Droits en jeu

- Droit à la protection des données
- Droit au respect de la vie privée

Question juridique

Est-il permis, lors d'une procédure de recrutement, de rechercher les candidat·e·s sur les réseaux sociaux ? Et l'employeur peut-il se fonder sur les informations ainsi trouvées pour établir son choix ?

Analyse juridique

L'un des aspects problématiques d'Internet est qu'une fois diffusées, les informations sont en principe accessibles à tous les internautes, et difficiles à supprimer. En mettant des informations en ligne, le risque est grand qu'elles finissent aussi sous les yeux de personnes auxquelles elles n'étaient pas du tout destinées, comme de potentiels employeurs. Les réseaux sociaux prévoient certes la possibilité de ne rendre visibles certaines informations et photographies qu'à certains groupes de personnes, mais bien des internautes n'y pensent pas.

Chaque personne a en principe le droit de déterminer elle-même quel usage sera fait des informations la concernant. Elle est ainsi libre de garder pour elle des informations relatives à sa vie privée et de ne les partager ni avec les pouvoirs publics ni avec d'autres personnes. En recherchant sur les réseaux sociaux des photographies et des informations privées sur Monsieur B., cette employée du service du personnel pourrait donc avoir porté atteinte à son droit à la protection des données et à son droit au respect de la vie privée.

En tant qu'entreprise privée, l'employeur potentiel n'est certes pas directement soumis aux obligations découlant des droits fondamentaux et des droits humains. Certaines dispositions de la loi sur le travail et du droit des obligations garantissent toutefois la protection de la vie privée du personnel (→ **notions fondamentales point 2.2.7**), et il est largement admis qu'elles s'appliquent déjà lors de la procédure de recrutement[140]. Ces dispositions précisent que les employeurs ne peuvent chercher et prendre en compte que les informations pertinentes pour déterminer l'aptitude d'une personne à occuper un emploi.

Ce principe est transposable à la recherche d'informations sur les réseaux sociaux. Des publications à caractère exclusivement privé ne sont pas de nature à permettre de tirer des conclusions sur l'aptitude professionnelle d'un individu. Il s'agit là de contenus destinés à être diffusés dans le cercle privé. Cette interdiction d'exploiter les informations ainsi glanées vaut aussi pour les résultats obtenus par une recherche sur Google[141].

Il n'en va pas de même des données publiées sur des réseaux sociaux professionnels tels que LinkedIn par des personnes en recherche d'emploi, car elles l'ont été afin de favoriser leur carrière professionnelle. Les employeurs potentiels peuvent donc prendre en compte ces données pour évaluer un dossier de candidature et en tirer des conclusions sur l'aptitude de la personne à répondre à leurs besoins[142].

Conclusions et recommandations

Durant la phase de recrutement, le personnel des ressources humaines ne peut prendre en compte une photographie publiée sur un réseau social privé, mais y est autorisé si elle a été diffusée sur un réseau social professionnel.

Si Monsieur B. souhaite éviter que des inconnus ou des employeurs potentiels puissent consulter ses comptes sur les réseaux sociaux, il doit indiquer, dans les paramètres de son compte, ce qui sera visible pour tous et ce qui ne

140 Pellascio, Kommentar zu Art. 328b, 2016, no 4.

141 Egli, Soziale Netzwerke und Arbeitsverhältnis, 2011, ch. marg. 79.

142 Egli, Soziale Netzwerke und Arbeitsverhältnis, 2011, ch. marg. 71 s. ; Streiff, von Kaenel et Rudolph, Arbeitsvertrag, 2012, Art. 328b, ch. marg. 9.

le sera pas. Il lui est aussi possible de supprimer les photographies qu'il a lui-même postées. S'il veut faire supprimer des images qui ont été publiées par une autre personne, il peut dans un premier temps demander à cette dernière de le faire et, si ceci n'aboutit pas, s'adresser à l'exploitant de la plateforme. S'il ne parvient toujours pas à ses fins, il lui reste la possibilité d'intenter une action civile pour exiger que les photographies soient supprimées.

Informations supplémentaires

Le droit de faire supprimer des données figure explicitement dans la loi sur la protection des données révisée, qui entrera prochainement en vigueur. C'est ce que l'on appelle le « droit à l'oubli numérique » (art. 32, al. 2, LPD rév.) : les informations concernant des personnes ne doivent pas être disponibles pour toujours sur Internet. La personne concernée doit avoir la possibilité de demander leur suppression lorsqu'aucun intérêt prépondérant ne s'y oppose[143].

L'OFCOM a publié un guide sur les possibilités à disposition des particuliers pour exiger la suppression des commentaires et photos postées sur les réseaux sociaux[144].

143 Conseil fédéral, Message sur la révision totale de la LPD, p. 6693.

144 OFCOM, Médias sociaux, 2013.

1.3 Surveillance au travail

Madame C., monteuse d'ascenseurs, utilise un véhicule d'entreprise lorsqu'elle est en service extérieur. Or, ce véhicule est depuis quelque temps équipé d'un GPS. Son mari, Monsieur C., est économiste d'entreprise et travaille en partie au bureau et en partie à domicile. Son employeur lui a fourni un ordinateur portable afin qu'il puisse faire du télétravail.

Madame C., qui se sent mal à l'aise à l'idée que le GPS permet à son employeur de savoir exactement où elle se rend et à quelle heure, aimerait qu'il soit désinstallé. Quant à Monsieur C., il se demande si cela pose problème qu'il envoie des courriels privés pendant son temps de travail depuis l'ordinateur portable que son employeur a mis à sa disposition.

Droits en jeu

- Droit au respect de la vie privée
- Liberté de mouvement
- Droit à la santé

Question juridique

À quelles conditions est-il licite d'utiliser des technologies de surveillance et de contrôle sur un lieu de travail ? Les employé·e·s peuvent-ils s'opposer à cette surveillance ?

Analyse juridique

Il existe de nombreuses technologies utilisables pour surveiller ou contrôler des processus au poste de travail : caméras de surveillance, systèmes de géolocalisation tels que GPS dans le cas de Madame C. ou technologie portable (montre intelligente, par ex.). Des logiciels permettent également de surveiller les activités auxquelles les employé·e·s, comme Monsieur C., peuvent s'adonner en ligne. Ces technologies peuvent servir à assurer la sécurité du personnel ou de tiers, à protéger la santé des individus ou à garantir la sécurité de biens revêtant une importance pour l'entreprise (comme

dans une bijouterie). Elles permettent toutefois aussi de contrôler les actes des membres du personnel, notamment afin d'optimiser le rendement et les processus.

Lorsqu'un employeur utilise des technologies pour surveiller ou contrôler ses employé·e·s, des données sur le comportement au travail de ces derniers sont saisies, collectées et, parfois, analysées[145]. Une telle pratique ne respecte pas leur droit à la vie privée. Et comme on peut aussi imaginer que les collaborateurs et collaboratrices, conscients de cette surveillance, ne se meuvent plus librement durant leurs heures de travail, cette surveillance limite aussi leur liberté de mouvement. Enfin, une surveillance constante peut en outre occasionner des problèmes de santé, et donc violer également le droit à la santé[146].

Contrairement aux pouvoirs publics, les employeurs privés ne sont pas directement tenus de respecter les droits fondamentaux et les droits humains. Leurs employé·e·s bénéficient néanmoins des dispositions de la loi sur la protection des données, de la loi sur le travail et du code des obligations, qui les protègent de toute violation de leurs droits fondamentaux et de leurs droits humains due à une surveillance dans le cadre d'un rapport de travail de droit privé (→ **notions fondamentales point 2.2.7**). Ces dispositions fixent des conditions précises pour le recours à des systèmes de surveillance et l'utilisation des données qu'ils collectent.

L'article 328b du code des obligations, qui relève du droit du travail, joue ici un rôle important, comme dans le cas pratique concernant les postulations et les réseaux sociaux : il dispose en effet que les employeurs ne peuvent récolter et analyser que les informations ayant un lien étroit avec le travail, comme des données sur les heures de travail effectuées ou la qualité de leurs prestations[147] ; ils doivent en outre respecter les principes de la loi sur la protection des données, qui exigent que tout traitement de données personnelles doit être licite et que leur destruction doit faire l'objet d'une réglementation[148]. De plus, il leur est interdit de recourir à des systèmes de surveillance ou de contrôle exclusivement pour surveiller les actes des tra-

145 Pärli, Kommentar DSG, 2015, Art. 328b OR, no 11.

146 SECO, Commentaire des ordonnances 3 et 4 Ltr, 2020, ch. marg. 326-1.

147 Streiff, von Kaenel et Rudolph, Arbeitsvertrag, 2012, Art. 328b OR, ch. marg. 6.

148 Pärli, Kommentar DSG, 2015, Art. 328b OR, no 15 s.

vailleurs et travailleuses à leur poste de travail (art. 26 OLTr 3). Et lorsque ces systèmes sont nécessaires pour des raisons de sécurité du personnel ou de contrôle du travail fourni, ils ne peuvent être utilisés que de manière à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleuses et travailleurs.

Selon la pratique actuelle, pour être licite, la surveillance au moyen d'outils technologiques doit être proportionnée et être justifiée par un intérêt clairement prépondérant de l'employeur (comme l'identification d'abus). Ce dernier doit en particulier la limiter autant que possible, aussi bien dans le temps que dans l'espace. De plus, il est tenu d'avertir le personnel de l'existence de cette surveillance et de l'associer à sa planification et à sa réalisation[149].

Le GPS installé dans le véhicule de service de Madame C. relève les mouvements du véhicule et permet donc de connaître les trajets effectués et leurs horaires, des données qui, à leur tour, fournissent certaines indications sur la durée de travail et les éventuelles pauses de cette employée. Du point de vue des employeurs, ces informations sont utiles en cela qu'elles permettent de mieux planifier les missions, de contrôler le personnel et aussi, par conséquent, d'éviter les abus. Il s'agit là, selon le Tribunal fédéral, de raisons légitimes pour installer un GPS dans un véhicule de service. Cette surveillance ne doit toutefois pas se faire en temps réel et doit concerner seulement les véhicules que les employé·e·s n'utilisent pas à des fins privées. Si ces conditions sont remplies, le recours à des logiciels de géolocalisation est en principe permis. Madame C. doit toutefois au préalable en avoir été informée, avoir donné son accord et, si possible, avoir été associée à la planification de cette surveillance[150].

Pour ce qui est de Monsieur C., les considérations juridiques sont les suivantes : c'est aux employeurs qu'il revient de déterminer si leur personnel est autorisé à envoyer des messages privés depuis l'ordinateur du bureau et à naviguer sur Internet à des fins privées pendant les heures de travail, et si oui, dans quelles limites. Les entreprises adoptent généralement un règlement d'utilisation pour fixer un cadre en la matière. Quant aux données

149 Meier-Gubser, Mitarbeiterüberwachung, 2020, p. 286 s.

150 Au sujet des conditions à respecter pour installer un GPS dans un véhicule de service : ATF 130 II 425.

secondaires (→ **notions fondamentales point 1.1**) des courriels envoyés durant le temps de travail, elles ne peuvent faire l'objet que d'une analyse anonymisée. En revanche, si l'employeur de Monsieur C. a de bonnes raisons de le soupçonner d'enfreindre le règlement ad hoc, il peut analyser les courriels suspects[151].

Conclusions et recommandations

La surveillance des trajets de Madame C. touche certes plusieurs droits fondamentaux et droits humains, mais devrait en principe être permise à la lumière de la jurisprudence actuelle. Les supérieur·e·s hiérarchiques de Madame C. doivent toutefois veiller à ce que le mal-être que génère en elle cette surveillance ne mette pas en péril sa santé psychique. Dans les cas qui ne remplissent pas les conditions pour que la surveillance soit licite, il est possible de demander conseil auprès de l'inspection cantonale du travail, un organe chargé de veiller au respect des dispositions de la loi sur le travail.

En ce qui concerne Monsieur C., c'est le règlement ad hoc de son employeur qui détermine dans quelle mesure il est autorisé à envoyer des courriels privés depuis l'ordinateur de son bureau.

Informations supplémentaires

Le cas de Madame C. est similaire à une affaire sur laquelle le Tribunal fédéral s'est prononcé (ATF 130 II 425). Les conditions à remplir pour avoir recours à des technologies de surveillance et de contrôle au travail figurent dans le commentaire que le SECO a publié concernant les ordonnances 3 et 4 relatives à la loi sur le travail[152]. Pour des explications détaillées sur la surveillance des courriels au poste de travail, on consultera le *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail* que le PFPDT a publié pour l'économie privée[153].

151 Hafner, Auswertung E-Mails, 2018, p. 1331 ss.

152 SECO, Commentaire des ordonnances 3 et 4 Ltr, 2020.

153 PFPDT, Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée), 2013.

2 Santé

2.1 Robots de soins

Monsieur D., qui souffre d'une démence avancée, vit dans un EMS géré par sa commune. Sa fille s'inquiète pour son bien-être, car cette institution utilise plusieurs robots dans la prise en charge générale et les soins à ses pensionnaires. Elle trouve particulièrement préoccupant que l'on recoure, pour amuser son père, à un robot bébé phoque nommé Rosa, une peluche dotée de capteurs, qui simule des interactions sociales avec Monsieur D.

Droits en jeu

- Dignité humaine
- Interdiction de toute peine ou tout traitement inhumain ou dégradant
- Droit à des conditions de travail équitables

Question juridique

Les robots de soins sont conçus entre autres pour aider les personnes prises en charge (en transportant pour elles de petits objets), pour soutenir le personnel soignant (en déplaçant des personnes, par ex.) et pour distraire, comme dans le cas du robot bébé phoque (→ **notions fondamentales point 1.7**). Le fait de confier à un robot de soins une partie de la prise en charge de Monsieur D., notamment pour le distraire, viole-t-il son droit à la dignité humaine ou l'interdiction des traitements inhumains ou dégradants ? Que pourrait faire Monsieur D. (ou, vu sa démence, sa fille) si le recours à un robot de soins l'inquiète ? Et que sait-on de l'effet de ces robots sur le droit du personnel soignant de jouir de conditions de travail équitables ?

Analyse juridique

Le principe de la dignité humaine veut que toute personne soit traitée en tout temps avec dignité, comme un individu ayant une valeur intrinsèque. Monsieur D. étant atteint de démence, il n'est plus forcément possible de savoir s'il se rend compte que Rosa, le bébé phoque, n'est pas un vrai animal,

mais un robot. S'il devait ne pas en être conscient, on simulerait donc une interaction avec un être vivant, ce qui serait problématique du point de vue de la dignité humaine.

Pour déterminer si l'utilisation d'un robot de service ou d'assistance respecte ou non la dignité humaine, il est possible de se référer à la formule dite de l'objet : selon celle-ci, la dignité humaine est bafouée lorsqu'on rabaisse une personne au rang d'objet. Or, des gestes de la vie courante comme le fait de porter une personne, de la laver ou de la faire passer d'un lit à un fauteuil par exemple génèrent d'ordinaire un contact physique et émotionnel entre elle et le personnel soignant. En présence de robots de soins, une partie de ces occasions de contact disparaissent et les soins se résument de plus en plus à un simple processus d'« entretien » semblable à ce qui se fait pour des objets. Le besoin fondamental de l'être humain d'éprouver des émotions authentiques, d'avoir des contacts sociaux et de toucher et d'être touché par d'autres personnes ne serait plus satisfait avec un robot de soins, ce qui pourrait aussi constituer une atteinte à la dignité humaine[154].

Pour déterminer si le recours à des robots de soins constitue un traitement inhumain ou dégradant, il faut avant tout savoir s'il y a souffrances physiques ou psychiques d'une certaine intensité durant un certain temps. Si les robots de service ou d'assistance sont utilisés de manière adéquate, on peut supposer que ce n'est pas le cas. De plus, diverses études sur ces robots bébés phoques ont montré qu'il est rare que les personnes prises en charge les rejettent, et qu'un éventuel rejet n'allait pas de pair avec des souffrances psychiques[155].

Pour ce qui est du personnel soignant, on peut imaginer que ces robots, en l'aidant à accomplir ses tâches, lui permettent de consacrer davantage de temps aux soins des pensionnaires et aux contacts humains avec eux. Dans ce cas, la qualité de la prise en charge s'en trouverait améliorée, et avec elle la qualité de vie des personnes aînées. Il est aussi possible que ces robots de soins épargnent certaines tâches physiquement pénibles au personnel. Ces aspects ne doivent cependant pas faire oublier que bien des soignant·e·s sont mal à l'aise à l'idée de devoir à l'avenir faire exécuter leur travail par des robots.

154 Kreis, Pflegeroboter, 2018, p. 222 ss.

155 Baisch, Kolling, Rühl et al., Emotionale Roboter, 2018.

Conclusions et recommandations

Le recours à des robots de soins ne respecte pas la dignité humaine lorsqu'il vise à remplacer en bonne partie les soins octroyés par des personnes et réduit pratiquement à zéro le contact humain avec le personnel. Ce serait par exemple le cas si un robot de divertissement était censé remplacer les relations que les soignant·e·s nouent avec les pensionnaires. Or, les contacts sociaux, et le droit qui s'y rapporte d'avoir de véritables sentiments et des contacts humains, sont un élément essentiel de la vie d'une personne. Différents types de robots peuvent par contre être mis en service comme soutien, sous la surveillance d'une personne soignante qui garantit l'indispensable contact social et physique. Dans le cas de Monsieur D., pour respecter ses droits, le personnel ne devrait pas le laisser seul avec le robot bébé phoque dans les bras, mais l'accompagner et le soutenir pendant cette utilisation. Il ne devrait pas non plus lui faire croire qu'il s'agit d'un animal en chair et en os.

Si la fille de Monsieur D. se fait du souci pour le bien-être de son père, elle peut dans un premier temps en parler avec le personnel et la direction de l'établissement. Certains cantons disposent par ailleurs d'un service de médiation pour les conflits en institutions, auquel elle peut aussi s'adresser.

Informations supplémentaires

Ce cas s'inspire de « Paro », un robot de divertissement développé au Japon pour la prise en charge des personnes atteintes de démence[156]. Ce type de robot a aussi été testé en Suisse[157].

156 Ammann, Robotergestützte Pflege, 2019.

157 SRF, Soziale Roboter in Altersheimen, 2020.

2.2 Diagnostics fondés sur l'intelligence artificielle et les mégadonnées

Madame E., qui présente depuis un certain temps des taches suspectes sur un bras, va consulter dans un hôpital universitaire. Une dermatologue prend des photographies de son bras, puis les fait analyser par un logiciel chargé de déterminer si les taches sont ou non dues à un cancer de la peau. Le test est négatif. Le logiciel en question est à la pointe de la recherche et tout le processus est reconnu par les milieux médicaux. Quelques semaines plus tard, une autre dermatologue diagnostique tout de même un cancer de la peau chez Madame E. Il s'avère alors que l'erreur de diagnostic commise par le logiciel s'explique par son jeu d'entraînement, constitué exclusivement de cancers de la peau détectés sur des individus de peau plus ou moins claire. Or, Madame E. ayant la peau plus foncée, le logiciel n'a pas pu y déceler son cancer.

Droits en jeu

- Droit à la santé
- Interdiction de la discrimination

Question juridique

Que peut-on dire, du point de vue des droits fondamentaux et des droits humains, sur le recours aux mégadonnées et à l'intelligence artificielle dans le domaine des diagnostics ?

Analyse juridique

Le droit à la santé exige de l'État qu'il garantisse les meilleurs soins possibles. Il se concrétise en particulier par le fait que les traitements doivent être à la pointe de la recherche et de la technique[158]. Ce principe s'applique aussi à l'utilisation de logiciels pour diagnostiquer une maladie, une technique qui peut aider les médecins dans leur travail. Ces logiciels sont capables d'exploiter d'importantes quantités de données provenant de toutes sortes de sources et le font de manière infiniment plus rapide que le personnel médi-

158 Widmer Lüchinger, Digitale Innovation und ärztliche Sorgfalt, 2019, p. 78 s.

cal. À cela s'ajoute le fait que les algorithmes sont souvent plus précis que les êtres humains[159]. Le recours à un logiciel constitue donc, en principe, un facteur favorable au droit à la santé.

L'utilisation de l'intelligence artificielle peut toutefois aussi enfreindre l'interdiction de discriminer. Si certains groupes de personnes ne sont pas suffisamment représentés dans les jeux de données utilisés pour concevoir et entraîner l'algorithme, il y a risque de discrimination, car le logiciel sera peut-être incapable de diagnostiquer une maladie chez les individus de ces groupes et se trompera systématiquement dans l'interprétation des symptômes. C'est ce qui s'est passé dans notre exemple : étant donné que le logiciel utilisé a été entraîné avec un jeu de données comprenant une grande majorité de personnes blanches, il n'est pas capable d'identifier le cancer de la peau chez les personnes de teint plus foncé.

Conclusions et recommandations

Dans ce cas pratique, il pourrait y avoir violation de l'interdiction de discriminer. Pour que le logiciel fournisse des diagnostics corrects, quelle que soit la couleur de peau des patient·e·s, les différentes couleurs de peau doivent être représentées à parts égales dans son jeu d'entraînement : celui-ci doit contenir dans une même mesure des images de cancer de la peau de chaque type de peau[160].

Informations supplémentaires

En Suisse, l'intelligence artificielle est utilisée dans de nombreux domaines pour établir des diagnostics, notamment du cancer du sein et du cancer du poumon[161].

---

159 Jannes, Friele, Jannes et al., Digitale Gesundheitsversorgung, 2018, p. 62.

160 Adamson/Smith, Machine Learning and health care disparities in dermatology, 2018 ; au sujet de la conception d'algorithmes du point de vue de l'interdiction de discriminer, voir aussi le → **cas pratique Un algorithme sélectionne les dossiers de candidature 1.1**.

161 NZZ, Diagnose vom Computer, 2019.

2.3 Capteur d'activité physique d'une caisse-maladie

Monsieur F. participe à un nouveau programme de bonus que sa caisse-maladie a lancé pour promouvoir le mouvement au quotidien : il porte un podomètre qui enregistre le nombre de ses pas et transmet ensuite ces données à l'assurance, via une application. Chaque jour durant lequel il dépasse les 10 000 pas lui donne droit à un bonus qui se transforme ensuite en une remise sur sa prime d'assurance.

Droits en jeu

- Droit à la santé
- Interdiction de la discrimination
- Droit au respect de la vie privée
- Droit à la protection des données

Question juridique

Est-il permis aux assurances d'octroyer aux assuré·e·s participant à un programme fondé sur un capteur d'activité physique une remise sur les primes de l'assurance-maladie de base et de l'assurance complémentaire ?

Analyse juridique

Les remises accordées sur les primes d'assurance-maladie dans le cadre de programmes recourant à des capteurs d'activité physique soulèvent des questions en lien avec le droit à la santé et l'interdiction de la discrimination. Quant au fait d'enregistrer des données sur l'activité physique de Monsieur F., il touche le droit au respect de la vie privée et le droit à la protection des données.

Le droit à la santé figure dans la Constitution fédérale en tant que but social, mais pas en tant que droit à faire valoir en justice. Ce sont la Confédération et les cantons qui doivent le réaliser, en faisant en sorte que chaque personne obtienne les soins nécessaires à sa santé (art. 41, al. 1, let. b Cst.). L'assurance de base obligatoire constitue à cet égard un élément central et dans ce domaine, les assurances-maladies sont tenues de respecter les droits fon-

damentaux[162] ainsi que divers principes de la loi sur l'assurance-maladie. Les caisses-maladie doivent admettre à l'assurance de base toute personne qui en fait la demande (obligation de contracter), une obligation qui ne s'applique pas à l'assurance complémentaire. De plus, elles ne sont pas autorisées à fixer leurs primes en fonction de l'état de santé ou d'une autre caractéristique de la personne assurée, telle que l'âge (principe de solidarité). Tous les personnes assurées d'une assurance-maladie domiciliées dans une même région paient par conséquent le même montant mensuel, à quelques exceptions près.

En proposant un programme de bonus semblable à celui de ce cas pratique, une assurance de base risque de remettre en question le principe de solidarité et d'enfreindre l'interdiction de discriminer. Des assuré·e·s jeunes ou en bonne santé pourraient obtenir des bonus grâce à leur activité physique et donc, en fin de compte, des remises sur leurs primes, ce qui pourrait pénaliser, dans l'assurance de base, les assuré·e·s âgés ou physiquement limités, par exemple. Les assurances de base ne sont donc pas autorisées à accorder, aux dépens des autres personnes assurées, des remises ou des bonus que la loi ne prévoit pas. Les programmes de bonus et les remises qui en découlent ne sont permis que s'ils ne sont ni proposés ni financés par l'assurance de base, mais par exemple par une société d'assurances complémentaires faisant partie de la même compagnie que l'assurance de base en question[163].

Quant aux assurances complémentaires, elles ne sont pas directement tenues de respecter les droits fondamentaux et le principe de solidarité inscrit dans la loi sur l'assurance-maladie (→ **notions fondamentales point 2.2.6**), mais il ne leur est pas pour autant permis d'accorder des remises illimitées dans le cadre de programmes d'enregistrement de l'activité physique. Les remises sont illicites si elles introduisent des inégalités de traitement entre personnes assurées et désavantagent certaines d'entre elles, sans que cela ne se justifie pour des raisons juridiques ou actuarielles (c'est-à-dire qui concernent l'assurance) (art. 117, al. 2 OS).

162 Rütsche, Was sind öffentliche Aufgaben?, 2013, p. 153.

163 Conseil national, interpellation 18.3282, Empêcher les atteintes au principe de solidarité dans l'assurance de base, réponse du Conseil fédéral du 1er juin 2018.

Conclusions et recommandations

Le bonus octroyé à Monsieur F. pour le récompenser de sa participation au programme n'est licite que si ce programme est proposé et financé par une société d'assurance complémentaire et que la remise ne constitue pas une inégalité de traitement illicite envers d'autres assuré·e·s. Un programme dont les bonus seraient financés par les primes de l'assurance de base contreviendrait à la loi.

Informations supplémentaires

Ce cas pratique s'inspire de l'arrêt 2C_717/2017 du 25 novembre 2019 du Tribunal fédéral et de l'arrêt A-3548/2018 du 19 mars 2019 du Tribunal administratif fédéral.

3 Démarches administratives, judiciaires et politiques

3.1 Des sites internet officiels accessibles

Une commune suisse présente sur son site internet ses activités et les prestations qu'elle offre à la population. Elle y met aussi à disposition des documents tels que des formulaires de demandes d'autorisation. Elle a reçu plusieurs plaintes au sujet de ce site : les personnes malvoyantes disent avoir de la peine à s'y retrouver et à lire les informations publiées. Une association de défense des droits des personnes porteuses d'un handicap mental a également fait part de ses griefs. Elle regrette que tous les contenus soient rédigés en langue standard et exige que la commune traduise au moins les informations et formulaires les plus importants en langue facile à lire.

Droits en jeu

- Liberté de l'information
- Interdiction de la discrimination

Question juridique

En communiquant sur un site internet peu clair et peu accessible, des autorités violent-elles la liberté de l'information et l'interdiction de la discrimination ? Existe-t-il un droit à des sites internet sans obstacles ?

Analyse juridique

La liberté de l'information comprend le droit de se procurer les informations accessibles à tout un chacun, et les informations des autorités entrent dans cette catégorie. Elle n'oblige pas les collectivités publiques à informer de leur propre gré la population de leur action, mais si elles le font, elles doivent veiller à respecter l'interdiction de la discrimination. De nombreux cantons

imposent par ailleurs un devoir d'information à leurs autorités cantonales : ces dernières sont alors tenues d'informer la population de toute action présentant un intérêt général[164] et de respecter l'interdiction de discriminer.

Les sites internet des pouvoirs publics doivent donc être conçus de manière à être accessibles à toutes les personnes intéressées[165]. Pour ce qui est des personnes porteuses de handicap[166], l'article 9 de la Convention des Nations Unies relative aux droits des personnes handicapées exige des États qu'ils prennent des mesures pour leur assurer, sur la base de l'égalité avec les autres, l'accès à l'information et aux prestations publiques. Elles doivent pouvoir accéder de manière autonome, sans frais supplémentaires, aux informations dont elles ont besoin et que leurs autorités ont publiées.

Toutes les autorités publiques fédérales, cantonales et communales doivent respecter ces dispositions. La loi fédérale sur l'élimination des inégalités frappant les personnes handicapées dispose par exemple que les autorités fédérales doivent prendre en considération les besoins particuliers des handicapé·e·s de la parole, de l'ouïe ou de la vue (art. 14 LHand) et que toutes les prestations que la Confédération propose sur Internet doivent être accessibles également aux personnes handicapées (art. 10 OHand). Des initiatives sont également prises à l'échelle cantonale ou communale : le canton de Zurich et la ville de Berne ont ainsi adapté leurs sites internet pour les rendre accessibles à toute le monde[167].

Les autorités fédérales, cantonales et communales sont par conséquent tenues de veiller à ce que leurs sites internet soient dépourvus d'obstacles. Une étude menée en 2016 a néanmoins montré que les sites de nombreux cantons et villes étaient encore trop peu accessibles aux personnes handica-

164 § 14 de la loi sur l'information et la protection des données du canton de Zurich (Gesetz über die Information und den Datenschutz) (LS 170.4).

165 Langer, Staatliche Nutzung von Social Media-Plattformen, 2014, p. 952.

166 La Convention des Nations Unies relative aux droits des personnes handicapées définit ces dernières comme « des personnes qui présentent des incapacités physiques, mentales, intellectuelles ou sensorielles durables dont l'interaction avec diverses barrières peut faire obstacle à leur pleine et effective participation à la société sur la base de l'égalité avec les autres.» Cette définition ne fait toutefois pas l'unanimité auprès des personnes concernées.

167 Regierungsrat Kanton Zürich, Digitale Verwaltung, 2020, p. 9 ; Gemeinderat Stadt Bern, Barrierefreiheit, 2018.

pées[168]. Dans le cas pratique présenté ici, le site internet de la commune ne remplit pas les exigences en matière d'accessibilité, puisque les personnes malvoyantes ne parviennent pas à télécharger les documents et que celles présentant un handicap mental ne les comprennent pas.

Conclusions et recommandations

Quand des obstacles empêchent les personnes handicapées d'accéder à d'importantes informations figurant sur les sites internet des autorités publiques, il peut y avoir, selon les circonstances, violation tant de l'interdiction de discriminer que de la liberté d'information. Les personnes porteuses de handicap ne peuvent certes pas saisir la justice pour exiger que tous les sites internet leur soient accessibles, mais si l'une d'entre elles ne parvient pas, en raison du caractère peu accessible d'un site, à bénéficier d'une prestation publique disponible sur Internet, elle pourrait dans certains cas porter son cas devant la justice[169].

Informations supplémentaires

Il existe de nombreuses possibilités de concevoir des sites internet de manière à ce que les personnes en situation de handicap aient accès aux informations qui s'y trouvent ou les comprennent. Des systèmes audios « lisent » les textes et les rendent par conséquent accessibles aux personnes malvoyantes. Pour les malentendant·e·s, il est possible d'ajouter des sous-titres aux vidéos. Enfin, la traduction en langage simplifié permet d'adapter les informations publiées aux personnes présentant un handicap mental ou des difficultés d'apprentissage : on reformule le message en se limitant à des phrases principales brèves et à des notions simples, de manière à ce qu'il soit nettement plus facile à comprendre[170].

---

168 Fondation suisse « Accès pour tous » pour une technologie adaptée aux handicapés, Étude Accessibility en Suisse, 2016.

169 Des organisations telles qu'Inclusion Handicap, la faîtière suisse des organisations de personnes handicapées, proposent des conseils juridiques aux personnes handicapées afin de faire respecter leurs droits.

170 BFEH, Communication numérique accessible, 2018, p. 1 s. ; BFEH, Fiche d'information Langue facile à lire, 2019.

3.2 Automatisation de décisions administratives

G., une brasserie suisse, est assujettie à l'impôt sur la bière et présente une déclaration d'impôt semestrielle. L'autorité fédérale compétente en la matière confie l'examen des informations transmises non pas à son personnel, mais à un logiciel qu'elle a fait développer pour cette tâche. Ce logiciel établit également la décision de taxation et la facture qui l'accompagne.

Droits en jeu

– Droit à une procédure équitable (et en particulier droit d'être entendu)

Question juridique

On parle de décision administrative entièrement automatisée lorsqu'une décision ou une ordonnance d'une autorité est rendue par un logiciel, sans aucune intervention humaine[171]. Que faut-il en conclure du point de vue du droit d'être entendu ?

Analyse juridique

Le droit d'être entendu signifie que toute partie doit avoir l'occasion de présenter ses arguments, de prendre connaissance de son dossier et de se prononcer à ce sujet. L'autorité doit quant à elle prendre en compte ces arguments et fonder suffisamment sa décision ou son arrêt. Or, en cas d'automatisation de la décision, il est difficile pour la personne administrée, voire impossible, de faire respecter ses droits, en l'absence de contact direct avec le service en question. De plus, une décision prise par un logiciel risque de ne pas prendre suffisamment en compte les circonstances concrètes du cas particulier[172].

Le législateur, conscient de la problématique des décisions administratives automatisées, a prévu une disposition à ce sujet lors de la révision de la loi sur la protection des données (art. 21 LPD rév.). Cette norme s'applique exclusivement aux décisions prises de manière entièrement automatisée, sans

171 Braun Binder, Anordnungen der Maschinen, 2020, p. 256.

172 Weber, Automatisierte Entscheidungen, 2020, p. 24 ; Rechtsteiner, Der Algorithmus verfügt, 2018, ch. marg. 19 s.

aucune intervention humaine tout au long du processus[173]. La décision de taxation automatisée présentée ci-dessus entrerait donc dans ce cas de figure.

La personne doit être informée que la décision la concernant a été prise de manière automatisée (art. 21, al. 1er, LPD rév.). Pour que son droit d'être entendue soit respecté, elle doit avoir la possibilité de faire connaître son point de vue et peut aussi exiger qu'un·e employé·e du service concerné examine la décision (art. 21, al 2, LPD rév.)[174].

Conclusions et recommandations

Une fois la révision de la loi sur la protection des données en vigueur, toute administration fiscale fédérale souhaitant rendre des décisions automatiques devra respecter les nouvelles dispositions de celle-ci. Dans notre cas pratique, l'administration fiscale en question devra, avec les nouvelles dispositions, informer l'entreprise G. que la décision de taxation la concernant a été prise de manière automatisée. De plus, elle devra garantir à G. la possibilité de prendre position durant la procédure et faire examiner la décision par un·e employé·e avant de la lui transmettre.

Informations supplémentaires

L'exemple présenté ici est fictif, mais, à l'occasion de la révision de la loi sur la protection des données, diverses lois fédérales ont été modifiées pour créer une base légale permettant aux autorités fédérales de prendre des décisions de taxation individuelles automatisées, notamment pour les droits de douane, la redevance sur le trafic poids lourds ainsi que pour l'impôt sur le tabac, celui sur la bière et celui sur les huiles minérales. Des dispositions analogues ont été adoptées dans le domaine de l'assurance-accident et de l'assurance militaire afin d'anticiper d'éventuelles évolutions.

173 Conseil fédéral, Message sur la révision totale de la LPD, p. 6673.

174 Braun Binder, Automatisierte Entscheidungen, 2020, p. 31.

3.3 Automatisation d'évaluations de risque

Depuis un certain temps, Monsieur H. harcèle et menace son ex-femme. Cette dernière ayant contacté la police, il est convoqué à un entretien avec une personne mandatée par le canton et formée pour réaliser des évaluations de risque. Les réponses de Monsieur H. sont ensuite transmises à la police et saisies dans un système qui, sur la base d'un algorithme, calcule sa probabilité de passer à l'acte et de devenir violent. Ce logiciel parvient à un risque de quatre points sur cinq.

Droits en jeu

- Droit à une procédure équitable (et en particulier droit d'être entendu et présomption d'innocence)
- Interdiction de la discrimination
- Droit à la liberté et à la sûreté

Question juridique

Monsieur H. estime que cette évaluation automatisée soulève des questions du point de vue de l'interdiction de la discrimination, de la présomption d'innocence et du droit à la liberté et à la sécurité.

Analyse juridique

Le programme utilisé dans ce cas pratique relève de la police prédictive, un processus lors duquel un logiciel contribue à préparer une décision administrative, qui est ensuite prise par un·e membre du service concerné.

Ce recours à un algorithme menace non seulement le droit d'être entendu, déjà abordé ci-dessus (→ **cas pratique Automatisation des décisions administratives 3.2**), mais pourrait aussi enfreindre l'interdiction de discriminer. Une décision administrative prise sur la base d'un algorithme peut de prime abord paraître plus objective que celle établie par un collaborateur ou une collaboratrice d'un service, puisque les décisions d'un individu sont influencées par ses expériences, ses valeurs et ses ressentis, forcément subjectifs. Un algorithme, pourrait-on penser, ne prend en compte que des données et des faits. Ce serait oublier qu'un algorithme a été créé par des

humains et que leurs opinions, préjugés et expériences sont intégrées dans le développement du logiciel. De plus, la décision de l'algorithme se base sur d'anciens cas qui ont également été traités par des individus, dont les valeurs ont par conséquent aussi influencé les données sur lesquelles se fonde le logiciel[175]. Le recours à un logiciel peut donc reproduire une éventuelle discrimination commise par le passé et même la renforcer, en raison du phénomène dit de la prophétie autoréalisatrice. Le programme étasunien COMPAS, qui calculait des risques de récidive deux fois plus élevés pour les Afro-Américain·e·s que pour les personnes blanches, illustre très bien ce mécanisme[176].

La présomption d'innocence comprend trois principes : toute personne suspectée est considérée comme innocente tant qu'elle n'a pas été condamnée ; c'est aux autorités pénales de prouver sa culpabilité ; enfin, les juges doivent traiter son cas de manière impartiale. Comme les techniques de police prédictive ne font qu'évaluer le risque d'un individu de perpétrer un délit et ne débouchent pas sur une condamnation a priori en raison d'un délit déjà commis, elles ne devraient pas entrer en conflit avec la présomption d'innocence[177].

Reste également à déterminer si l'on pourrait ordonner une mise en détention préventive (art. 221, al. 2, CP) sur la base d'une évaluation de risque automatisée. Selon la Convention européenne des droits de l'homme (art. 5, al. 1er, let. c), il est permis de priver un individu de sa liberté s'il présente un danger concret de mettre à exécution une menace de perpétrer un grave délit et si la détention préventive est ordonnée avec une grande réserve[178].

Conclusions et recommandations

Plusieurs conditions doivent être remplies pour qu'une évaluation de risque automatisée respecte les droits fondamentaux et les droits humains. D'une part, toute décision automatisée telle que la police prédictive doit se fonder sur une base légale ; actuellement, le recours à cette technologie est souvent

175 Thouvenin, Früh et George, Automatisierte Entscheidungen, 2018, ch. marg. 9.

176 NZZ, Algorithmen unter Rassismusverdacht, 2016.

177 Camavdic, Predictive Policing in der Schweiz, 2019, ch. marg. 14.

178 Schmid et Jositsch, Kommentar zu Art. 221 StPO, 2018, no 14 ; Hug et Scheidegger, Kommentar zu Art. 221 StPO, 2014, no 40 ss.

justifié par la clause générale de police, c'est-à-dire le devoir de la police de prévenir les délits. D'autre part, pour respecter l'interdiction de discriminer, le jeu de données qui a servi à entraîner l'algorithme doit refléter la diversité de la société et respecter le principe de transparence[179] (→ **cas pratique Un algorithme sélectionne les dossiers de candidature 1.1** et **cas pratique Diagnostics fondés sur l'intelligence artificielle et les mégadonnées 2.2**).

Informations supplémentaires

En Suisse, on recourt de plus en plus fréquemment à des logiciels pour prédire et prévenir les graves actes de violence : la police convoque à un entretien les individus chez qui on observe certains signaux d'alarme précis, déterminés au préalable par la recherche scientifique, qui laissent conclure à un risque de passage à l'acte. Les résultats de cet entretien ainsi que d'autres informations, tirées par exemple des dossiers de ces individus, sont saisis dans un logiciel. Un algorithme établit alors le risque d'acte de violence et le programme fait une première évaluation, puis c'est l'autorité compétente qui décide si la personne en question doit être considérée comme une menace ou pas[180].

179 Braun Binder, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, 2019, p. 473.

180 Simmler, Brunner et Schedler, Smart Criminal Justice, 2020, p. 14 ss ; Conseil fédéral, La gestion des menaces, 2017, p. 5 ss.

3.4 Microciblage durant des campagnes politiques

Madame I. souhaite s'informer sur Internet au sujet des prochaines votations. Après une rapide recherche, elle tombe sur le site internet d'un parti et y lit ses prises de position sur les différents objets soumis au vote. À l'ouverture de ce site, elle a cliqué sur la fenêtre qui s'est affichée et a déclaré accepter les cookies. Peu de temps après, elle découvre en ouvrant son compte Facebook une annonce publicitaire du parti en question au sujet des futures votations. Elle se sent observée, ce qui la met mal à l'aise.

Droits en jeu

- Liberté d'opinion
- Droits politiques (droit à la libre formation de l'opinion en particulier)
- Droit au respect de la vie privée
- Droit à la protection des données

Question juridique

Que peut-on dire, du point de vue des droits fondamentaux et des droits humains, du microciblage lors de campagnes électorales et campagnes de votations ? Ce parti politique avait-il le droit de transmettre les données de Madame I. à Facebook ?

Analyse juridique

Les campagnes politiques ne se mènent plus seulement dans le monde analogique, mais aussi dans le monde numérique. En rendant les échanges très faciles, les réseaux sociaux jouent en effet un rôle important dans la formation de l'opinion sur les sujets politiques. Les campagnes numériques peuvent toutefois porter atteinte aux droits fondamentaux et aux droits humains. Le fait de diffuser des contenus par microciblage durant une campagne de votation (→ **notions fondamentales point 1.2**) touche en particulier la liberté d'opinion et la libre formation de l'opinion politique. Quant au fait de collecter et d'analyser des données pour identifier des groupes cibles, il soulève des questions sur le droit au respect de la vie privée et celui à la protection des données.

La liberté d'opinion comprend notamment le droit de se forger son opinion politique, de l'exprimer et de la diffuser librement. Le microciblage est l'une des nombreuses méthodes auxquelles les partis politiques et les groupes d'intérêt ont le droit de recourir pour diffuser leurs points de vue et leurs messages. Selon le Tribunal fédéral, ce n'est que dans des cas exceptionnels que la liberté d'opinion peut être limitée dans le domaine politique[181]. Ce serait par exemple le cas si des propos racistes étaient diffusés au moyen du microciblage.

La Constitution fédérale exige que les résultats des votations et des élections soient l'expression fidèle et sûre de la volonté des citoyen·ne·s. Pour cela, il faut que les votant·e·s aient été informés de manière correcte et équilibrée, tant par les pouvoirs publics que par les entités privées ou les particuliers[182]. Des stratégies de communication particulièrement agressives qui, via le microciblage, diffusent de manière ciblée sur les réseaux sociaux des informations partiales au sujet d'objets soumis aux citoyen·ne·s seraient donc susceptibles de porter atteinte à la libre formation de l'opinion. Dans un tel cas, les autorités seraient tenues d'intervenir dans la campagne et de rectifier les informations. Quant à la suspension d'une votation ou d'une élection, elle ne serait envisageable que dans des circonstances exceptionnelles[183].

Le microciblage comprend aussi la collecte et l'analyse d'importants volumes de données personnelles, ce qui soulève des questions par rapport au respect de la vie privée et à la protection des données. Même si ce sont des entités privées (partis politiques, entreprises spécialisées) qui exploitent ces données, et non des pouvoirs publics, et qu'elles ne sont donc pas directement liées par les droits fondamentaux et les droits humains, les internautes ne sont toutefois pas démunis, car ils sont protégés par la loi sur la protection de données (→ **notions fondamentales point 2.2.7**).

Les votant·e·s ont, en vertu des dispositions relatives à la protection des données, le droit de savoir quelles méthodes et technologies de traitement numérique des données sont utilisées pour les contacter et les influencer politiquement. Étant donné que les informations concernant les activités et intérêts politiques entrent dans la catégorie des données sensibles, la col-

181 ATF 131 IV 23 consid. 3.1.
182 ATF 121 I 138 consid. 3.
183 ATF 135 I 292 consid. 4.

lecte et la transmission de ces données ne sont permises que si elles sont clairement identifiables par la personne concernée et que cette dernière y a expressément donné son accord (art. 4, al. 5 LPD ; art. 6, al. 6 et 7 LPD rév.). Un parti politique par exemple, qui souhaite collecter les données des internautes qui visitent son site pour ensuite les combiner avec d'autres données afin d'établir des profils de microciblage, n'est autorisé à le faire que si la personne concernée en a été suffisamment informée et qu'elle a donné librement et expressément son accord. Ce consentement peut par exemple être donné en cochant une case à part, en plus de l'accord de principe concernant les cookies (le fait d'accepter les conditions générales d'utilisation ne suffit pas). De plus, les internautes doivent être informés de manière complète et facilement compréhensible de la façon dont leurs données seront traitées. Il est notamment obligatoire de leur faire savoir que leurs données seront combinées avec des données tirées des réseaux sociaux, si c'est le cas. En outre, ils doivent pouvoir à tout moment révoquer leur consentement et demander la suppression de leurs données[184].

Conclusions et recommandations

Plusieurs droits fondamentaux et droits humains sont concernés par le recours au microciblage durant les campagnes politiques. Du point de vue de la liberté d'opinion et des droits politiques, cette méthode de communication politique est en principe acceptable. Toutefois, étant donné le gros volume de données collectées et traitées ainsi que l'établissement de profils de personnalité spécifiques, elle porte atteinte à la vie privée et au droit à la protection des données. C'est, comme nous l'avons vu ci-dessus, la loi sur la protection des données qui fixe dans quelles conditions le traitement de données à des fins de microciblage est permis.

Dans le cas pratique présenté ici, la transmission des données de Madame I. est illicite. Cette dernière n'a en effet pas été suffisamment informée du fait que ses données seraient combinées avec d'autres données tirées des réseaux sociaux et ne pouvait donc pas donner expressément son accord (par exemple en cliquant sur une fenêtre à part). Son consentement général à l'utilisation de cookies ne suffit pas. Madame I. peut en principe demander la suppression des données qui ont été transmises sans son accord, mais cette

184 PFPDT et Privatim, Guide relatif aux élections et votations, 2019.

démarche se révèle souvent difficile. Elle a également la possibilité, comme pour toute question relevant de la protection des données, de demander conseil au bureau du Préposé fédéral à la protection des données et à la transparence (PFPDT).

Informations supplémentaires

Cet exemple est inspiré des élections fédérales 2019, lors desquelles plusieurs partis politiques ont transféré à Facebook les données des internautes ayant visité leurs sites internet, parfois sans leur consentement. Ces personnes ont par la suite reçu des publicités ciblées des partis en question. Une fois ces faits révélés, les partis ont été plus transparents au sujet tant de la transmission des données que du consentement à ce sujet[185].

Des explications détaillées sur le microciblage lors des campagnes de votation et d'élection sont disponibles dans le Guide des autorités de protection des données de la Confédération et des cantons[186].

185 SRF, CVP verschweigt digitalen Datenspion, 2019.

186 PFPDT et Privatim, Guide relatif aux élections et votations, 2019.

3.5 Vidéosurveillance étatique avec reconnaissance faciale dans l'espace public

Madame J., qui milite au sein des jeunes pour le climat, participe régulièrement à des manifestations pacifiques. Elle a lu dans plusieurs médias que certains pays pratiquent la vidéosurveillance avec reconnaissance faciale lors de gros rassemblements tels que manifestations ou évènements sportifs. Elle se demande ce qu'il en est en Suisse et à quelles conséquences elle doit s'attendre en tant que participante à des rassemblements autorisés.

Droits en jeu

- Liberté de réunion
- Liberté d'opinion (liberté d'expression en particulier)
- Liberté de mouvement
- Droit au respect de la vie privée
- Droit à la protection des données

Question juridique

Que peut-on dire de la vidéosurveillance avec reconnaissance faciale (→ **notions fondamentales point 1.4**) dans l'espace public du point de vue des droits fondamentaux et des droits humains ? En Suisse, l'État est-il autorisé à installer des caméras de surveillance dotées de reconnaissance faciale dans l'espace public ?

Analyse juridique

La liberté d'expression et la liberté de réunion garantissent à chaque personne le droit de participer à des manifestations pacifiques et d'y exprimer son opinion. Or, le fait de participer à un rassemblement révèle souvent quelque chose de nos opinions politiques ou de nos caractéristiques personnelles (comme notre orientation sexuelle), tout en nous garantissant un certain anonymat au milieu de la foule. Cet anonymat, et la protection qui en découle, disparaissent toutefois si l'espace public où se tient le rassemblement est doté de caméras de surveillance et s'il n'est pas exclu que des logiciels de reconnaissance faciale identifient les participant·e·s. En cas de doute, bien des personnes pourraient renoncer à participer à une manifes-

tation pour ne pas courir le risque de voir leurs données collectées, en particulier celles concernant leurs opinions politiques. Cette surveillance limiterait par conséquent indirectement la liberté d'expression et la liberté de réunion (c'est ce que l'on appelle l'effet de dissuasion ou d'intimidation, ou encore le *chilling effect*)[187].

La vidéosurveillance avec reconnaissance faciale peut aussi limiter de manière indirecte la liberté de mouvement. Elle n'empêche certes pas directement un individu de se mouvoir librement dans l'espace public, mais s'il ne souhaite pas être filmé ou identifié dans un certain endroit, il devra alors l'éviter[188].

Enfin, le recours à des logiciels de reconnaissance faciale dans l'espace public constitue aussi une atteinte au respect de la vie privée et au droit à la protection des données. Chaque personne a en principe le droit de déambuler dans l'espace public sans être observée. Or, d'importantes quantités de données personnelles sont collectées lorsque la police filme des personnes. Pour respecter les droits fondamentaux et les droits humains, le recours à un logiciel de reconnaissance faciale doit donc absolument réunir trois conditions : reposer sur une base légale, servir l'intérêt public et être proportionnel.

Si des caméras permettant la reconnaissance faciale étaient installées dans bon nombre d'espaces publics, on serait en présence d'une surveillance de masse. Les données de nombreuses personnes seraient collectées sans soupçon concret envers une personne précise, ce qui n'est pas admissible du point de vue des droits fondamentaux et des droits humains. Le fait de pouvoir savoir qui a fait quoi, où et à quel moment restreint considérablement la vie privée, la liberté d'opinion et la liberté de réunion[189]. Il est vrai qu'au moment de l'enregistrement de ces images, la personne concernée peut tout à fait n'y voir aucun problème. Mais si les pouvoirs publics conservent ces données durant un certain temps et finissent par établir un

187 Haut-Commissariat des Nations Unies aux droits de l'homme, New technologies in the context of assemblies, 2020, ch. marg. 34.

188 Schweizer, Kommentar zu Art. 10 BV, 2014, no 35.

189 Weydner-Volkmann et Feiten, Vertrauensstiftende Videoüberwachung ?, 2019, p. 218.

lien entre ce lieu et une orientation politique déterminée, par exemple, le fait de s'être fait filmer à cet endroit précis risque de devenir malgré tout problématique.

Conclusions et recommandations

Actuellement, les pouvoirs publics suisses ne sont pas autorisés à pratiquer la vidéosurveillance de l'espace public au moyen de logiciels de reconnaissance faciale. Pour pouvoir le faire, ils devraient adopter une nouvelle loi spécifique qui en précise les principaux aspects (but de la surveillance, suppression des données recueillies, etc.). De plus, ils devraient aussi systématiquement vérifier la proportionnalité de cette mesure avant de l'appliquer.

Informations supplémentaires

Différents pouvoirs publics pratiquent la reconnaissance faciale dans l'espace public. C'est le cas notamment de la police du Pays de Galles du Sud[190] ou de celle de Hambourg, qui l'a fait pour élucider des délits lors des manifestations contre le sommet du G20 en 2017[191].

En Suisse, la police des frontières utilise des logiciels de reconnaissance faciale à l'aéroport de Zurich lors du contrôle automatique des passeports des ressortissant·e·s de l'espace UE/AELE. Les douaniers et douanières ne s'en servent pas pour chercher à identifier des personnes inconnues, mais pour contrôler que la personne entrant dans notre pays est effectivement celle figurant dans le document d'identité présenté. Le logiciel procède à ce contrôle en se fondant sur les données biométriques du passeport. Aucune donnée n'est collectée à cette occasion[192].

190 Jugement de la Cour d'appel de Londres, R. contre Chief Constable of South Wales Police, 11.8.2020 (affaire numéro C1/2019/2670).

191 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, G20-Ermittlungen, 2020.

192 Kamasa, Grenzkontrollen in Europa, 2019.

4 Utilisation d'Internet

4.1 Commentaires haineux sur Internet

Madame K. fait partie d'une association qui vise à déconstruire les idées reçues sur l'islam. Elle est active notamment sur les réseaux sociaux, où elle publie régulièrement des billets sur les préjugés dont sont victimes au quotidien les personnes musulmanes. Chacune de ses contributions suscite de nombreux partages et réactions. Et parmi ces dernières, des commentaires racistes et des menaces de violence.

Droits en jeu

- Liberté d'opinion
- Dignité humaine
- Interdiction de la discrimination
- Liberté de conscience et de croyance

Question juridique

Comment saisir la justice pour dénoncer des discours de haine diffusés sur Internet ?

Analyse juridique

On entend généralement par discours de haine des commentaires haineux racistes, antisémites ou fondés sur un autre type d'intolérance[193]. Toute personne a en principe le droit d'exprimer librement son opinion. Cette liberté d'opinion s'étend en règle générale aussi aux commentaires publiés sur Internet, mais elle n'est pas absolue. Les commentaires haineux portent en effet atteinte à la dignité humaine, à l'interdiction de la discrimination et à la

193 Comité des Ministres du Conseil de l'Europe, Discours de haine, 1997.

liberté de conscience et de croyance. La liberté d'opinion des individus peut donc être limitée afin de préserver les droits fondamentaux et les droits humains d'autrui[194].

Les commentaires appelant publiquement à la haine ou à la discrimination envers des personnes en raison de leur « race »[195], de leur ethnie, de leur religion ou de leur orientation sexuelle sont punis par la loi, tout comme le fait de rabaisser des personnes ou de les discriminer en raison de l'une de ces caractéristiques, d'une façon qui porte atteinte à la dignité humaine (art. 261bis CP). Les commentaires haineux diffusés sur les réseaux sociaux sont normalement considérés comme publics et tombent donc sous le coup de cette interdiction pénale.

Les commentaires haineux fondés sur d'autres motifs, comme ceux contre les femmes ou les personnes âgées, ne sont pas considérés par le code pénal comme des incitations à la haine, mais tombent sous le coup d'autres dispositions pénales (concernant l'injure, la menace ou la contrainte, par ex.).

Conclusions et recommandations

Comme toute personne découvrant un commentaire haineux sur Internet, Madame K. a la possibilité de déposer plainte pénale auprès de la police. Cette dernière et le ministère public doivent alors mener une enquête pénale afin de voir si le commentaire en question contrevient à l'article 261bis du code pénal ou à une autre disposition pénale. Madame K. peut aussi exiger la suppression du commentaire (→ **cas pratique Cyberharcèlement 4.2**).

Informations supplémentaires

Il n'est pas toujours facile de savoir si un commentaire blessant publié sur Internet doit être considéré comme un discours de haine ou pas. Le site internet de la Commission fédérale contre le racisme présente un recueil de dé-

194 Hart, Hate-Speech, 2018, p. 20.

195 La notion de « race » figure dans le code pénal et la Constitution fédérale. Comme il s'agit là d'une construction sociale à la base même du racisme, la Commission fédérale contre le racisme recommande de mettre ce terme entre guillemets.

cisions et d'arrêts concernant l'article 261bis CP. Sous la rubrique « Moyens utilisés », sous « Communication électronique », on trouve des exemples concrets de procédures au sujet de discours de haine diffusés sur Internet.

4.2 Cyberharcèlement

L. est une gymnasienne de 17 ans. Elle se fait régulièrement injurier et importuner par ses camarades de classe et ce harcèlement s'étend rapidement aux réseaux sociaux, où circulent notamment des photographies d'elle prises dans la sphère privée. Pour L., la situation n'est plus supportable.

Droits en jeu

- Droit à l'intégrité psychique
- Liberté d'opinion

Question juridique

Que peut-on faire en cas de cyberharcèlement ?

Analyse juridique

Le fait d'injurier, de menacer ou de harceler systématiquement une personne par smartphone ou sur Internet durant un certain temps constitue du cyberharcèlement. Contrairement aux injures ou menaces proférées dans le monde analogique, les propos diffusés sur Internet y restent souvent accessibles pour une durée indéfinie. Ils sont de plus susceptibles d'être lus par un nombre considérablement plus important de personnes[196]. Le cyberharcèlement pouvant violer le droit à l'intégrité psychique, la liberté d'opinion ne s'étend donc normalement pas aux propos qui entrent dans cette catégorie[197].

Le code pénal suisse n'interdit pas spécifiquement le cyberharcèlement, mais plusieurs autres dispositions pénales, prévues à l'origine pour le monde analogique, s'appliquent aux commentaires publiés sur L. Il pourrait ainsi être question, entre autres, de diffamation (art. 173 CP), d'injure (art. 177 CP), de menace (art. 180 CP) et de contrainte (art. 181 CP). Certains

196 Brun, Cyberbullying, 2016, p. 101 s.

197 Au sujet du conflit entre, d'une part, la liberté d'opinion et, d'autre part, la protection de l'intégrité psychique et d'autres droits fondamentaux, voir le → **cas pratique Commentaires haineux sur Internet 4.1**.

de ces délits ne font l'objet d'une enquête que si la victime porte plainte (délits poursuivis sur plainte, comme la diffamation). D'autres doivent être poursuivis dès que la police ou le ministère public en ont connaissance, qu'il y ait ou non dépôt de plainte pénale (délits poursuivis d'office, comme la contrainte).

En cas de cyberharcèlement, il y a souvent aussi atteinte à la personnalité (art. 28 CC ss). Pour L., cela signifie qu'elle peut exiger que les commentaires injurieux ou menaçants et les photographies soient retirées des réseaux sociaux et, selon la situation, qu'une réparation pour tort moral ou des dommages-intérêts lui soient versés.

Conclusions et recommandations

Plusieurs entités offrent un premier conseil et un soutien aux victimes de cyberharcèlement (des centres scolaires, Pro Juventute, les centres de consultation LAVI d'aide aux victimes, par ex.). L. peut en contacter une pour voir quelle suite elle peut donner à son cas. Elle a en principe la possibilité de déposer plainte pénale dans les trois mois, auprès de la police.

Souvent, la victime de harcèlement ne tient pas seulement à faire condamner les coupables, mais aussi à faire supprimer les commentaires blessants. Si L. ne parvient pas à faire en sorte que l'exploitant du réseau social le fasse, elle peut déposer plainte auprès du tribunal civil de son lieu de domicile.

Informations supplémentaires

Des informations et des conseils plus détaillés au sujet du cyberharcèlement sont disponibles dans le fascicule publié par la Prévention suisse de la criminalité[198] ainsi que sur le site internet de Pro Juventute.

198 Prévention suisse de la criminalité, Cyberharcèlement, 2017.

5 Éducation et recherche

5.1 Enseignement scolaire en ligne

M. a 13 ans. Comme tous les autres enfants en âge de scolarité, il a suivi l'école à la maison lorsque les écoles ont dû fermer leurs portes en raison de la pandémie de Covid-19. Il recevait une partie de l'enseignement par visioconférence ainsi que des devoirs d'anglais à faire en ligne sur la version numérique de son livre d'école. Ses frères et sœurs suivaient eux aussi des cours en ligne et M. a dû partager avec eux le vieil ordinateur portable de leurs parents. Il n'a donc pu assister qu'aux deux tiers environ de ses cours et n'a pu faire qu'une partie de ses devoirs.

Droits en jeu

- Droit à l'éducation
- Droit à un enseignement de base suffisant

Question juridique

Quel est l'impact de la numérisation sur le droit à l'éducation ? Les cours en ligne sont-ils à même de garantir le droit à un enseignement de base inscrit dans la Constitution fédérale ? Compte tenu de sa situation particulièrement difficile, M. aurait-il eu droit à un soutien ?

Analyse juridique

Le potentiel des technologies numériques pour promouvoir l'éducation et, par conséquent, pour renforcer le droit à l'éducation est considérable : les enseignant·e·s peuvent avoir recours à des didacticiels pour améliorer la qualité de l'enseignement en classe ou pour le rendre entièrement virtuel, de façon à ce qu'il puisse être dispensé partout. Toutefois, les progrès de la numérisation dans le domaine de l'éducation peuvent aussi mettre à mal l'égalité des chances, lorsque certains élèves ne disposent pas des infrastructures requises (comme un accès suffisant à Internet et un ordinateur), des connaissances techniques nécessaires ou d'un environnement social favo-

rable[199]. Ainsi, selon le Baromètre de l'école pour la Suisse, l'Allemagne et l'Autriche, les enseignant·e·s n'ont pas pu établir de contact via des outils numériques avec un nombre considérable d'élèves durant la fermeture des écoles au printemps 2020. En outre, quelque 10 % des enfants et adolescents interrogés ont indiqué avoir eu des difficultés à suivre l'enseignement en ligne par manque d'appareils appropriés[200].

Le Comité des droits de l'enfant des Nations Unies s'est penché sur les liens entre les droits humains et la numérisation et technicisation de l'enseignement. Dans son observation générale consacrée à cette thématique, il enjoint aux États de garantir à tous les enfants l'accès aux technologies numériques indispensables à leur éducation. Les enseignant·e·s doivent par ailleurs dispenser un soutien suffisant (par d'autres moyens si besoin) aux enfants qui n'ont pas accès aux outils requis ou qui ne bénéficient pas de l'appui nécessaire de la part de leurs parents[201].

Dans notre exemple, reste à savoir si le droit de M. à un enseignement de base suffisant a été préservé en dépit des restrictions. Chaque enfant vivant en Suisse peut faire valoir en justice son droit à un enseignement de base suffisant et gratuit de la première enfantine à la troisième année d'école secondaire. La jurisprudence du Tribunal fédéral n'indique toutefois pas clairement si ce droit minimal peut être limité (à part en cas d'exclusions temporaires pour des motifs disciplinaires, qui sont jugées licites[202]). La mission de l'enseignement de base est de concrétiser l'égalité des chances : tous les enfants vivant en Suisse doivent recevoir au moins l'éducation dont ils ont besoin pour s'épanouir et agir plus tard en adultes responsables. Dès lors, l'enseignement de base n'est pas suffisant lorsqu'il ne dispense pas à l'enfant des connaissances indispensables pour la vie en société et lorsque l'égalité des chances est compromise[203].

199 Rapporteur spécial des Nations Unies sur le droit à l'éducation, Droit à l'éducation à l'ère numérique, 2016, ch. marg. 26 ss et 31 ss.

200 Huber, Günther, Schneider et al., COVID-19 Herausforderungen in Schule und Bildung, 2020, p. 25 s. et 83 s.

201 Comité des droits de l'enfant des Nations Unies, Observation générale no 25, ch. marg. 102 ss. ; Comité des droits de l'enfant des Nations Unies, Conséquences de la pandémie de COVID-19 sur les enfants, 2020, ch. marg. 3.

202 ATF 129 I 12.

203 ATF 129 I 12, consid. 4.1 s.

Conclusions et recommandations

Le droit de M. à un enseignement de base suffisant a été respecté si la limitation due au manque d'infrastructures ne le prive pas de connaissances essentielles pour son avenir, ce qui le mettrait en position d'inégalité par rapport à ses camarades et contreviendrait au principe de l'égalité des chances. Diverses mesures auraient dû être adoptées pour éviter cette situation : soit l'école aurait dû mettre un ordinateur ou une tablette à la disposition de M., soit l'enseignant·e aurait dû lui fournir la matière des cours sur papier et des explications par téléphone. Par ailleurs, l'école devrait, après la réouverture des classes, lui permettre de rattraper tout retard pris dans l'apprentissage en lui dispensant des cours d'appui.

Informations supplémentaires

Fournir (et donc financer) les appareils nécessaires aux élèves est une question cruciale en matière de numérisation en milieu scolaire. La Conférence suisse des directeurs cantonaux de l'instruction publique, qui en est pleinement consciente, a l'intention de formuler prochainement des recommandations concernant la fourniture des appareils requis aux élèves[204].

204 CDIP, Mesures relatives à la stratégie numérique, 2019, p. 4 s.

5.2 Publication d'une étude scientifique

Madame N. est employée d'une université. Dans le cadre d'une étude scientifique sur le placement d'enfants, elle réalise des entretiens avec des enfants placés et leurs parents biologiques, entretiens dont elle analyse ensuite le contenu. Le Fonds national suisse de la recherche scientifique, qui finance l'étude, exige notamment que les résultats et les données soient publiées, sous forme certes anonymisée, mais en libre accès.

Droits en jeu

- Liberté de la recherche
- Droit de bénéficier du progrès scientifique
- Droit au respect de la vie privée
- Protection des enfants et des jeunes
- Droit à la protection des données

Question juridique

De quelles règles particulières faut-il tenir compte concernant les données collectées, si ces dernières ainsi que les résultats d'une recherche doivent être publiés en libre accès ?

Analyse juridique

En 2017, le Fonds national suisse et l'association Swissuniversities ont décidé, dans le cadre de leur stratégie nationale de publications en libre accès (« open access »), que tous les résultats d'une recherche financée par des fonds publics seraient accessibles en ligne, gratuitement et sans restriction[205]. En vertu de cette décision, les résultats d'une étude doivent être publiés sous forme d'article dans une revue en libre accès ou dans un ouvrage en libre accès, par exemple. En outre, les données dont sont tirés les résultats doivent aussi être rendues publiques dans une base de données numérique (Open Research Data) conforme aux principes FAIR (facile à trouver, accessible, interopérable et réutilisable).

205 FNS, Règlement relatif à l'encouragement des publications en libre accès, 2017.

La publication en libre accès des études scientifiques sur Internet met en opposition plusieurs droits humains et droits fondamentaux : d'une part, le libre accès favorise la liberté de la recherche, puisque les chercheurs et chercheuses peuvent utiliser sans restriction les données et les résultats de travaux déjà réalisés dans leur discipline ou dans une autre discipline afin d'approfondir le sujet étudié. Le libre accès promeut par ailleurs l'échange entre scientifiques, ce qui améliore la qualité de la recherche, et renforce aussi le droit de tout individu de bénéficier du progrès scientifique et de ses applications. Chaque personne peut par exemple s'informer elle-même de l'état de la recherche dans un domaine déterminé et se prononcer à ce sujet.

D'autre part, le libre accès soulève la question du respect de la vie privée et du droit à la protection des données pour les personnes qui participent comme « sujets » à des projets scientifiques. Le recours à l'anonymisation n'écarte pas totalement le risque que ces personnes puissent être identifiées sur la base des données et des résultats publiés sur Internet. Ce risque est particulièrement élevé pour les données qualitatives (fichiers audio ou comptes rendus d'entretiens, par ex.), pour lesquelles la publication des données originales est d'ordinaire incompatible avec les codes éthiques en matière d'anonymisation[206].

Dès lors, les chercheurs et chercheuses doivent observer de nombreuses règles pour protéger les données des personnes participant aux études. Il leur faut d'une part respecter les lois sur la protection des données en vigueur là où ils réalisent leurs recherches : les lois cantonales s'ils travaillent dans une haute école suisse ou un hôpital public, la loi fédérale s'ils travaillent dans d'autres établissements ou à l'une des EPF ; à quoi s'ajoute le règlement général sur la protection des données s'ils participent aux programmes « Horizon » de l'Union européenne ainsi que d'autres exigences formulées par les bailleurs de fonds. Ainsi, le Fonds national suisse pose certes le principe du libre accès aux jeux de données des projets de recherche qu'il soutient, mais prévoit aussi des exceptions, notamment pour préserver les données personnelles sensibles. De surcroît, les chercheurs et chercheuses doivent expliquer dans un plan détaillé (appelé plan de gestion des données) la façon dont les données sont collectées et enregistrées et l'endroit où elles sont stockées, comme l'exige le principe de la reconnaissa-

206 Rocher, Hendrickx et de Montjoye, Re-identifications, 2019.

bilité inscrit dans la loi sur la protection des données[207]. Ils doivent en outre indiquer la manière dont ils résolvent les questions éthiques soulevées par la publication des données ainsi que le lieu et le format dans lesquels elles seront publiées. Enfin, ils sont tenus, pour certains objets d'étude, de demander une autorisation à l'une des commissions d'éthique cantonales ou universitaires.

Conclusions et recommandations

La protection des données pose un défi aux chercheurs et chercheuses, surtout lorsqu'ils sont obligés de rendre accessibles les données et les résultats de leurs études. Ils doivent en effet concilier au mieux les exigences du droit de la protection des données et les prescriptions de leurs institutions et des bailleurs de fonds. Les universités et les hautes écoles spécialisées disposent de services qui les conseillent sur ces questions.

Informations supplémentaires

Les sites internet du PFPDT, des préposés cantonaux à la protection des données et des hautes écoles fournissent de plus amples informations sur la gestion des données des recherches scientifiques en général et sur les données en libre accès en particulier.

207 Thouvenin, Forschung, Big Data und Datenschutzrecht, 2017, p. 42 s.

6 Économie

6.1 Magasin automatique

Entrant dans un magasin situé dans une gare, Monsieur O. s'étonne de l'absence de personnel à la caisse. Les client·e·s doivent déposer leurs achats dans une boîte équipée de capteurs qui saisissent automatiquement les articles choisis. Avant leur premier achat, les client·e·s doivent s'enregistrer. Pour ce faire, le magasin prend une photo numérisée de leur visage et établit une connexion en ligne avec leur compte bancaire. À chaque passage à la caisse, le client ou la cliente doit de nouveau se laisser scanner le visage et le montant correspondant aux articles choisis est débité de son compte.

Droits en jeu

- Droit au respect de la vie privée
- Droit à la protection des données

Question juridique

Quelles questions l'automatisation des magasins soulève-t-elle par rapport à la loi sur la protection des données ?

Analyse juridique

Un exploitant d'un magasin automatique collecte et mémorise diverses données de sa clientèle : d'une part le nom, les coordonnées bancaires et, éventuellement, l'adresse, ainsi que les produits achetés ; d'autre part les données biométriques obtenues grâce à la numérisation du visage. Les données biométriques sont des données personnelles sensibles.

Dans le cas qui nous occupe, ce n'est pas l'État, mais une entreprise qui traite des données. La loi sur la protection des données impose à quiconque traitant des données de respecter la vie privée et le droit à la protection des

données (→ **notions fondamentales point 2.2.7**), et fixe à quelles conditions des particuliers et des entreprises peuvent traiter les données d'autres particuliers (art. 26 ss. LPD ; art. 30 ss. LPD rév.).

L'entreprise qui collecte, mémorise et analyse des données personnelles doit veiller à ne pas porter une atteinte illicite à la personnalité de ses client·e·s, ce qui est le cas en particulier si elle traite leurs données sans leur consentement alors que ce dernier est requis par la loi. Le consentement est considéré comme valable si et seulement si la personne concernée l'a donné librement et après avoir été suffisamment informée. Dans un magasin entièrement automatisé, les client·e·s doivent consentir à la saisie de leurs données s'ils veulent y faire des achats. Et comme les données biométriques sont des données sensibles, ils doivent donner leur consentement de manière explicite. Il n'est en particulier pas suffisant que les client·e·s décochent des cases préalablement cochées : ils doivent eux-mêmes cocher ces cases afin d'accepter les dispositions relatives à la protection des données[208].

Plus les prestations automatisées seront répandues, plus il sera permis de douter que le client ou la cliente puisse consentir « librement » au traitement de ses données. Pour être libre, un consentement doit notamment avoir été donné sans avoir subi de pressions[209]. Lorsque certaines prestations ne peuvent plus être obtenues que par des canaux numériques, et contre la transmission de données personnelles, les consommateurs et consommatrices n'ont plus réellement le choix, ce qui, pour des prestations essentielles, soulève des questions en lien avec la protection des données.

Le traitement de données personnelles doit aussi remplir une série de conditions supplémentaires : il doit être effectué conformément aux principes de la bonne foi et de la proportionnalité et se limiter aux données utiles et nécessaires au but poursuivi par la collecte. Ces deux principes s'appliquent aussi à la conservation des données[210]. Par ailleurs, les données personnelles ne peuvent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. En outre, la personne concernée doit pouvoir se rendre compte que des données personnelles sont collectées et reconnaître le but dans lequel elles le sont. L'en-

208 Keller, Datenschutz, 2019, p. 45.

209 Baeriswyl, Kommentar zu Art. 4 DSG, 2015, no 65 s.

210 Baeriswyl, Kommentar zu Art. 4 DSG, 2015, no 20 ss.

treprise qui collecte des données doit aussi en vérifier l'exactitude et rectifier ou effacer les données erronées. Autre exigence de la loi, les données collectées doivent être protégées contre tout accès non autorisé. Enfin, ce n'est qu'en présence de motifs sérieux qu'il est permis de traiter des données personnelles ou de transmettre des données sensibles à des tiers contre la volonté de la personne. L'existence d'un intérêt privé ou public prépondérant constitue un juste motif (c'est le cas, par exemple, lors d'une enquête menée par la police dans le cadre de poursuites pénales).

Conclusions et recommandations

La légalité ou l'illégalité de la collecte et de l'enregistrement des données personnelles dans un magasin automatique dépend en particulier des informations fournies au client ou à la cliente lors du premier enregistrement, des données collectées, du but de la collecte, du mode de mémorisation des données et des éventuels autres usages qui en sont faits. La clientèle devrait par ailleurs savoir si le magasin a l'intention de se servir des données collectées pour lui adresser de la publicité ciblée. La numérisation du visage entraînant la collecte de données biométriques, le consentement explicite des client·e·s est requis.

Les client·e·s dont des données ont été recueillies de façon illicite peuvent demander à l'entreprise qu'elle les rectifie ou les efface. Ils peuvent si nécessaire introduire une action auprès d'un tribunal civil (art. 15, al. 1, LPD / art. 32, al. 2, LPD rév. en relation avec art. 28 CC).

Informations supplémentaires

En 2019, Migros a ouvert un magasin pilote à la gare centrale de Zurich : les client·e·s y accèdent grâce à une application avec laquelle ils paient ensuite eux-mêmes leurs achats. Dans d'autres pays, l'accès aux magasins automatiques se fait par le biais d'un logiciel de reconnaissance faciale[211].

211 NZZ, Der kassenlose Laden kommt in die Schweiz, 2019.

6.2 Modèles d'affaires en ligne (économie des plateformes)

Monsieur P. travaille comme coursier pour un service de livraison de repas à domicile géré sur une plateforme numérique. La plateforme l'informe via une application mobile du moment où il peut prendre un repas commandé chez un restaurateur pour aller le livrer. Monsieur P. est rémunéré à l'heure. Voilà qu'il tombe malade de la grippe et ne peut pas travailler durant une semaine : il ne touche alors pas de rémunération.

Droits en jeu

- Liberté économique
- Droit à des conditions de travail équitables
- Droit à la sécurité sociale

Question juridique

Ces derniers temps, les modèles d'affaires de l'économie dite des plateformes ont défrayé la chronique en raison notamment de la précarité des personnes qui y sont actives : on reproche aux exploitants des plateformes de traiter à tort leurs coursiers et coursières comme des indépendant·e·s et de les priver ainsi des avantages que le droit du travail et le droit des assurances sociales garantissent aux personnes salariées. Les exploitants des plateformes sont-ils libres de décider si les personnes qui y travaillent sont des salarié·e·s ou des « partenaires » indépendants ? Et que peut faire Monsieur P. s'il veut s'opposer à sa perte de gain ?

Analyse juridique

Le service de livraison décrit ci-dessus applique le modèle d'affaires de l'économie des plateformes : il met en contact fournisseurs et clients sur une place de marché numérique. Dans le cas qui nous occupe, l'exploitant met en lien clientèle, restaurants et coursiers : sur une application, les client·e·s peuvent passer commande auprès de certains restaurants et la plateforme attribue ensuite les services de livraison aux coursiers et coursières en ayant recours à un algorithme. L'exploitant encaisse des commissions sur chaque commande effectuée sur sa plateforme.

Les exploitants de plateformes qui proposent des services tels que la livraison de repas à domicile peuvent invoquer la liberté économique. Ils sont donc en principe libres de s'organiser et de conclure des contrats comme ils l'entendent. Ils peuvent ainsi engager les coursiers et coursières ou les mandater en tant qu'indépendant·e·s. Toutefois, la liberté économique n'est pas absolue et peut être restreinte, par exemple pour protéger les salarié·e·s.

La distinction entre le statut de salarié et celui de « partenaire » indépendant est importante puisqu'elle détermine la protection octroyée par le droit du travail et par les assurances sociales. En effet, le code des obligations contient plusieurs dispositions qui protègent les salarié·e·s, mais pas les indépendant·e·s. Il établit par exemple des délais de congé et l'obligation, en cas de maladie, de continuer à verser le salaire durant un certain temps. En revanche, le contrat passé avec un·e indépendant·e peut généralement être résilié avec effet immédiat et ne prévoit pas de droit à une rémunération en cas de maladie. Les personnes salariées bénéficient aussi de meilleures conditions pour ce qui est des assurances sociales : certaines d'entre elles leur sont en principe réservées et excluent par conséquent les indépendant·e·s (assurance-chômage, assurance-accidents sociale et prévoyance professionnelle obligatoire). Et dans le cas de l'AVS et de l'AI, les salarié·e·s et les employeurs se répartissent les cotisations à parts égales, tandis que les personnes indépendantes s'en chargent seules.

Une personne est considérée comme salariée en particulier lorsqu'elle est sous les ordres d'un employeur, fournit un travail pour un temps déterminé ou indéterminé et n'a pas à supporter le risque économique propre à un entrepreneur. La façon dont les rapports sont définis dans le contrat n'a aucune importance, c'est la caisse de compensation compétente qui tranche si une personne a ou non le statut de salarié, en examinant chaque cas sur la base des critères mentionnés ci-dessus[212].

Dans le cas qui nous occupe, la plateforme donne à Monsieur P. des instructions concernant les heures et les lieux auxquels il doit aller chercher et livrer les repas. C'est l'algorithme de la plateforme qui décide à quel coursier ou quelle coursière confier la livraison d'une commande déterminée. Sans ces instructions, Monsieur P. ne pourrait pas fournir ses services de coursier et

212 Caisse fédérale de compensation, Statut au regard du droit des assurances sociales, 2017.

ne gagnerait rien. Cette relation de dépendance est un sérieux indice établissant le statut de salarié de Monsieur P. Il pourrait donc invoquer les dispositions du droit du travail et aurait droit au versement de son salaire pendant sa maladie[213].

Conclusions et recommandations

La distinction entre le statut d'indépendant et le statut de salarié n'est pas toujours évidente, car elle dépend de l'organisation de l'entreprise. Il peut par conséquent aussi être difficile de faire valoir les prétentions découlant du droit du travail, comme le droit à la poursuite du versement du salaire en cas de maladie pour Monsieur P. Les coursiers et coursières dans la situation de Monsieur P. peuvent s'informer notamment auprès des services de conseil des tribunaux civils de première instance de leur canton.

Informations supplémentaires

En juin 2020, le Tribunal administratif de Genève a décidé que le service de livraison de repas à domicile « Uber Eats » était un employeur et a reconnu le statut de salarié aux coursiers et coursières[214].

213 Gächter et Meier, Rechtsgutachten Uber-Fahrer, 2018, ch. marg. 40 et 113.

214 NZZ, Uber, 2020.

Résumé

Comme le montrent les exemples de cas présentés dans cet ouvrage, la numérisation a d'importantes conséquences pour les droits fondamentaux et les droits humains et cela, dans les domaines les plus variés. Entreprises, pouvoirs publics et particuliers doivent en être conscients au moment de développer des technologies numériques, d'en inclure dans leurs processus, d'en utiliser ou d'avoir un contact quelconque avec elles. La numérisation n'est pas un phénomène incontrôlable, mais une évolution de la société qu'il est possible d'influencer et même de façonner. Il est donc essentiel de débattre de la manière dont les divers acteurs doivent concevoir, appliquer et, le cas échéant, réglementer les technologies numériques afin qu'elles ne restreignent pas les droits fondamentaux et les droits humains mais qu'elles contribuent plutôt à renforcer les garanties accordées à chaque individu.

Liste des abréviations

Al.	Alinéa
Art.	Article
ATF	Arrêt du Tribunal fédéral
BFEH	Bureau fédéral de l'égalité pour les personnes handicapées
CC	Code civil suisse
CDIP	Conférence suisse des directeurs cantonaux de l'instruction publique
CEDH	Convention européenne des droits de l'homme
ch. marg.	Chiffre marginal ou chiffres marginaux
CO	Code des obligations
Consid.	Considérant
CP	Code pénal
CPP	Code de procédure pénale
CSDH	Centre suisse de compétence pour les droits humains
Cst.	Constitution fédérale de la Confédération suisse
Éd.	Éditeurs·trices
EPF	École polytechnique fédérale
et al.	et autres (collaborateurs et collaboratrices)
FAZ	Frankfurter Allgemeine Zeitung
FNS	Fonds national suisse
GVP	Gerichts- und Verwaltungspraxis des Kantons Zug (Jurisprudence judiciaire et administrative du canton de Zoug)
IA	Intelligence artificielle
IdO	Internet des objets
InTeR	Zeitschrift zum Innovations- und Technikrecht (revue)
LCD	Loi fédérale contre la concurrence déloyale
LDA	Loi fédérale sur le droit d'auteur et les droits voisins

LEg	Loi sur l'égalité entre femmes et hommes
Let.	Lettre
LPD	Loi fédérale sur la protection des données
LPD rév.	Loi sur la protection des données (révisée)
NZZ	Neue Zürcher Zeitung
OCDE	Organisation de coopération et de développement économique
OFCOM	Office fédéral de la communication
OLTr 3	Ordonnance 3 relative à la loi du travail
OS	Ordonnance sur la surveillance des entreprises d'assurance privées
Pacte I ONU	Pacte international relatif aux droits économiques, sociaux et culturels
Pacte II ONU	Pacte international relatif aux droits civils et politiques
PFPDT	Préposé fédéral à la protection des données et à la transparence
PJA	Pratique juridique actuelle (revue)
RDS	Revue de droit suisse
RGPD	Règlement général sur la protection des données de l'Union européenne
RJB	Revue de la société des juristes bernois
RPS	Revue pénale suisse
RSDA	Revue suisse de droit des affaires et du marché financier
RSJ	Revue suisse de jurisprudence
SECO	Secrétariat d'État à l'économie
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
USS	Union syndicale suisse

Bibliographie

Abegg Andreas, Bernauer Christof, Welchen neuen Regulierungsbedarf schaffen Airbnb, Uber & Co.?, AJP/PJA 1/2018, p. 82 ss.

Adamson Adewole, Smith Avery, Machine Learning and Health Care Disparities in Dermatology, JAMA Dermatology 11/2018.

Akkaya Gülcan, Grund- und Menschenrechte in der Sozialhilfe, Ein Leitfaden für die Praxis, Lucerne 2015.

Akkaya Gülcan, Belser Eva Maria, Egbuna-Joss Andrea, Jung-Blattmann Jasmin, Grund- und Menschenrechte von Menschen mit Behinderungen, Ein Leitfaden für die Praxis der sozialen Arbeit, Lucerne 2016.

Ammann Robert, Nutzen und Grenzen der robotergestützten Pflege, Krankenpflege/ Soins infirmiers 4/2019, p. 22 ss.

Baeriswyl Bruno, Kommentar zu Art. 4 DSG, in : Baeriswyl Bruno, Pärli Kurt (Éd.), Stämpflis Handkommentar zum Datenschutzgesetz, Berne 2015.

Baisch Stefanie, Kolling Thorsten, Rühl Saskia et al., Emotionale Roboter im Pflegekontext, Empirische Analyse des bisherigen Einsatzes und der Wirkung von Paro und Pleo, Zeitschrift für Gerontologie und Geriatrie 1/2018, p. 16 ss.

Bezemek Christoph, The 'Filter Bubble' and Human Rights, in : Petkova Bilyana, Ojanen Toumas (Éd.), Fundamental Rights Protection Online, The Future Regulation of Intermediaries, Cheltenham 2020, p. 34 ss.

Biaggini Giovanni, BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2e édition, Zurich 2017.

Bitkom e.V., DFKI, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, Berlin 2017.

Braun Binder Nadja, Als Verfügungen gelten Anordnungen der Maschinen im Einzelfall : Dystopie oder künftiger Verwaltungsalltag?, RDS 139/2020, p. 253 ss.

Braun Binder Nadja, Automatisierte Entscheidungen, Perspektive Datenschutzrecht und öffentliche Verwaltung, RSDA 1/2020, p. 27 ss.

Braun Binder Nadja, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, RSJ 115/2019, p. 467 ss.

Breitenmoser Stephan, Schweizer Rainer J., Kommentar zu Art. 13 BV, in : Ehrenzeller Bernhard, Schindler Benjamin, Schweizer Rainer J. et al. (Éd.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3e édition, Zurich 2014.

Brun Marcel, Cyberbullying – aus strafrechtlicher Sicht, recht – Zeitschrift für juristische Weiterbildung und Praxis 2/2016, p.100 ss.

Büchler Andrea, Kommentar zu Art. 28 ff. ZGB, in : Kren Kostkiewicz Jolanta, Wolf Stephan, Amstutz Marc et al. (Éd.), ZGB Kommentar, 3e édition, Zurich 2016.

Camavdic Benjamin, Predictive Policing in der Schweiz, Die Vereinbarkeit des Predictive Policing mit der schweizerischen Rechtsordnung, Jusletter IT, 26.9.2019.

Cavelti Urs Josef, Kley Andreas, Kommentar zu Art. 15 BV, in : Ehrenzeller Bernhard, Schindler Benjamin, Schweizer Rainer J. et al. (Éd.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3e édition, Zurich 2014.

Dastin Jeffrey, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, 11.10.2018.

Diggelmann Oliver, Kommentar zu Art. 13 BV, in : Waldmann Bernhard, Belser Eva Maria, Epiney Astrid (Éd.), Basler Kommentar Bundesverfassung, Bâle 2015.

Eggen Mirjam, Home Smart Home, Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, AJP/PJA 9/2016, p. 1131 ss.

Eggen Mirjam, Stengel Cornelia, Wearables – Eine vertragsrechtliche Betrachtung, Jusletter, 19.11.2018.

Egger, Dreher & Partner AG, Bestandesaufnahme aller arbeitsmarktlichen Massnahmen für über 50-jährige Stellensuchende in den Kantonen, 17.4.2019.

Egli Sandra, Egbuna-Joss Andrea, Ghielmini Sabrina, Belser Eva Maria, Kaufmann Christine, Grundrechte im Alter, Ein Handbuch, Lucerne 2019.

Egli Urs, Soziale Netzwerke und Arbeitsverhältnis, Über die Auswirkung von Facebook, Xing & Co. auf den betrieblichen Alltag, Jusletter, 17.1.2011.

Errass Christoph, Kommentar zu Art. 22 BV, in : Ehrenzeller Bernhard, Schindler Benjamin, Schweizer Rainer J. et al. (Éd.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3e édition, Zurich 2014.

FAZ Online, Eine Blockchain für den Schwarzen Seehecht, 16.10.2019.

Fondation suisse « Accès pour tous » pour une technologie adaptée aux handicapés, Étude Accessibility 2016 en Suisse, Zurich 2016.

Gächter Thomas, Meier Michael E., Sozialversicherungsrechtliche Qualifikation von Uber-Fahrern, Rechtsgutachten zuhanden der UNIA Bern, Zurich 2018.

Glatthaar Matthias, Robot Recruiting, Datenschutzrechtliche Aspekte einer Automatisierung von Rekrutierungsentscheiden, RSDA 1/2020, p. 43 ss.

Gyarmati Nikolaus, Phänomen Cybercrime und seine Bekämpfung, SZK 1/2019, p. 86 ss.

Hafner Peter, Auswertung der E-Mails von Arbeitnehmern, AJP/PJA 11/2018, p. 1327 ss.

Hart Patrick, Hate-Speech, Ein sozialpsychologisches Phänomen im Zeitalter der Globalisierung, in : Grafl Christian, Klob Bernhard, Reindl-Krauskopf Susanne (Éd.), „Das wird man ja wohl noch sagen dürfen!" – Meinungsfreiheit und Strafrecht, Schriftenreihe Kriminalwissenschaften in Theorie und Praxis 12/2018, p. 13 ss.

Hattenhauer Rainer, Das Computerlexikon für Einsteiger, Bonn 2019.

Huber Stephan Gerhard, Günther Paula Sophia, Schneider Nadine et al., COVID-19 – aktuelle Herausforderungen in Schule und Bildung, Erste Befunde des Schul-Barometers in Deutschland, Österreich und der Schweiz, Münster 2020.

Hug Markus, Scheidegger Alexandra, Kommentar zu Art. 221 StPO, in : Donatsch Andreas, Hansjakob Thomas, Lieber Viktor (Éd.), Kommentar zur Schweizerischen Strafprozessordnung, Zurich 2014.

Jannes Marc, Friele Minou, Jannes Christiane et al., Algorithmen in der digitalen Gesundheitsversorgung, Gütersloh 2018.

Jiang Fei, Jiang Yong, Zhi Hui et al., Artificial intelligence in healthcare, Past, present and future, Stroke and Vascular Neurology 2/2017, p. 230 ss.

Jørgensen Rikke Frank, Human Rights and Private Actors in the Online Domain, in : Land Molly K., Aronson Jay D. (Éd.), New Technologies for Human Rights Law and Practice, Cambridge 2018, p. 243 ss.

Kägi-Diener Regula, Kommentar zu Art. 19 BV, in : Ehrenzeller Bernhard, Schindler Benjamin, Schweizer Rainer J. et al. (Éd.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3e édition, Zurich 2014.

Kälin Walter, Künzli Jörg, Universeller Menschenrechtsschutz, Der Schutz des Individuums auf globaler und regionaler Ebene, 4e édition, Bâle 2019.

Kamasa Julian, Neue Technologien für Grenzkontrollen in Europa, CSS Analysen zur Sicherheitspolitik 255/2019, p. 1 ss.

Keller Claudia, Datenschutz, Zurich 2019.

Kiener Regina, Kälin Walter, Wyttenbach Judith, Grundrechte, 3e édition, Berne 2018.

Kreis Jeanne, Umsorgen, überwachen, unterhalten – sind Pflegeroboter ethisch vertretbar?, in : Bendel Oliver (Éd.), Pflegeroboter, Wiesbaden 2018, p. 213 ss.

Langer Lorenz, Staatliche Nutzung von Social Media-Plattformen, AJP/PJA 7/2014, p. 946 ss.

Markić Luka, Die elektronische Stimmabgabe im Lichte des Prinzips der Öffentlichkeit, E-Voting im Spannungsverhältnis zwischen dem Ruf nach mehr digitaler Demokratie und der Wahl- und Abstimmungsfreiheit, in : Dal Molin-Kränzlin Alexandra, Schneuwly Anne Mirjam, Stojanovic Jasna (Éd.), Digitalisierung – Gesellschaft – Recht, APARIUZ 2019, p. 125 ss.

Meier-Gubser Stefanie, Mitarbeiterüberwachung, Rechte, Pflichten und Verbote, TREX 5/2020.

Möhring Katja, Naumann Elias, Reifenscheid Maximiliane et al., Die Mannheimer Corona-Studie, Schwerpunktbericht zu Erwerbstätigkeit und Kinderbetreuung, Mannheim 2020.

Müller Jörg Paul, Verwirklichung der Grundrechte nach Art. 35 BV, Der Freiheit Chancen geben, Berne 2018.

NZZ, Algorithmen unter Rassismusverdacht, 24.5.2016.

NZZ, Die Diagnose kommt vom Computer, 26.7.2019.

NZZ, Der kassenlose Laden kommt in die Schweiz – wird bald auch Gesichtserkennung eingesetzt?, 27.8.2019.

NZZ, Uber muss nachgeben : In Genf haben die Food-Kuriere nun einen Arbeitsvertrag, 1.9.2020.

Pärli Kurt, Kommentar zu Art. 328b OR, in : Baeriswyl Bruno, Pärli Kurt (Éd.), Stämpflis Handkommentar zum Datenschutzgesetz, Berne 2015.

Pellascio Michel, Kommentar zu Art. 328 ff. OR, in : Kren Kostkiewicz Jolanta, Wolf Stephan, Amstutz Marc et al. (Éd.), OR Kommentar, 3e édition, Zurich 2016.

Raso Filippo, Hilligoss Hanna, Krishnamurthy Vivek et al., Artificial Intelligence & Human Rights, Opportunities & Risks, Berkman Klein Center Research Publication 6/2018.

Rechsteiner David, Der Algorithmus verfügt, Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, Jusletter, 26.11.2018.

Rocher Luc, Hendrickx Julien M., de Montjoye Yves-Alexandre, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications 10/2019, p. 1 ss.

Rütsche Bernhard, Was sind öffentliche Aufgaben?, recht – Zeitschrift für Weiterbildung und Praxis 4/2013, p. 153 ss.

Schafheitle Simon, Weibel Antoinette, HR Tech Survey, Pulse of people analytics in Switzerland 2020, Saint-Galle 2020.

Schmid Niklaus, Jositsch Daniel, Praxiskommentar Schweizerische Strafprozessordnung, 3e édition, Zurich/Saint-Gall 2018.

Schweizer Rainer J., Kommentar zu Art. 10 BV, in : Ehrenzeller Bernhard, Schindler Benjamin, Schweizer Rainer J. et al. (Éd.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3e édition, Zurich 2014.

Simmler Monika, Brunner Simone, Schedler Kuno, Smart Criminal Justice, Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege, Saint-Gall 2020.

Söbbing Thomas, Künstliche Intelligenz im HR-Recruiting-Prozess, Rechtliche Rahmenbedingungen und Möglichkeiten, InTeR 2/2018, p. 64 ss.

Sprecher Franziska, Datenschutzrecht und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, RJB 8/2018, p. 519 ss.

SRF, CVP verschweigt digitalen Datenspion, 26.6.2019.

SRF, Aargauer und Solothurner Polizei bleiben bei Autonummern-Scanner, 31.10.2019.

SRF, Wie soziale Roboter in Altersheimen helfen sollen, 15.10.20.

Streiff Ullin, von Kaenel Adrian, Rudoplh Roger, Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7e édition, Zurich 2012.

Tagesanzeiger, Lieferroboter der Post fahren nicht mehr, 4.3.2019.

Thouvenin Florent, Forschung im Spannungsfeld von Big Data und Datenschutzrecht, Eine Problemskizze, in : Boehme-Nessler Volker, Rehbinder Manfred (Éd.), Big Data, Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Berne 2017, p. 27 ss.

Thouvenin Florent, Früh Alfred, George Damian, Datenschutz und automatisierte Entscheidungen, Jusletter, 26.11.2018.

Tschannen Pierre, Kommentar zu Art. 33 BV, in : Waldmann Bernhard, Belser Eva Maria, Epiney Astrid (Éd.), Basler Kommentar Bundesverfassung, Bâle 2015.

USS, Dossier 125 : La numérisation doit servir les salarié(e)s, Berne 2017.

Vallone Vera, Wenn sich Algorithmen absprechen, Wettbewerbsabreden durch künstliche Intelligenz, ex ante 2/2018, p. 35 ss.

Weber Rolf H., Thouvenin Florent (Éd.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zurich 2014.

Weber Rolf H., Laux Christian, Oertly Dominic, Datenpolitik als Rechtsthema, Zurich 2016.

Weber Rolf H., Blockchain als rechtliche Herausforderung, Jusletter, 18.5.2017.

Weber Rolf H., Thouvenin Florent, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, RSD 1/2018, p. 43 ss.

Weber Rolf H., Digitalisierung und der Kampf ums Recht, in : Dal Molin-Kränzlin Alexandra, Schneuwly Anne Mirjam, Stojanovic Jasna (Éd.), Digitalisierung – Gesellschaft – Recht, APARIUZ 2019, p. 3 ss.

Weber Rolf H., Automatisierte Entscheidungen, Perspektive Grundrechte, RSDA 1/2020, p. 18 ss.

Wermelinger Amédéo, Kommentar zu Art. 15 DSG, in : Baeriswyl Bruno, Pärli Kurt (Éd.), Datenschutzgesetz (DSG), Berne 2015.

Weydner-Volkmann Sebastian, Feiten Linus, Vertrauensstiftende Videoüberwachung?, digma 4/2019, p. 218 ss.

Widmer Lüchinger Corinne, Digitale Innovation und ärztliche Sorgfalt, Life Science Recht – Juristische Zeitschrift für Pharma, Biotech und Medtech 2/2019, p. 77 ss.

Wildhaber Isabelle, Robotik am Arbeitsplatz, Robo-Kollegen und Robo-Bosse, AJP/PJA 2/2017, p. 213 ss.

Wirth Felix, Johns Marco, Meurers Thierry et al., Anonymisierung medizinischer Daten, Innovative medizinische Forschung benötigt qualitativ hochwertige Daten. Können diese sicher anonymisiert werden?, digma 2/2020, p. 74 ss.

Wohlers Wolfgang, Kommentar zu Art. 79b StGB, in : Wohlers Wolfgang, Godenzi Gunhild, Schlegel Stephan (Éd.), Handkommentar Schweizerisches Strafgesetzbuch, 4e édition, Berne 2020.

Zeit Online, Twitter-Nutzer machen Chatbot zur Rassistin, 24.3.2016.

Zeller Franz, Kiener Regina, Kommentar zu Art. 17 BV, in : Waldmann Bernhard, Belser Eva Maria, Epiney Astrid (Éd.), Basler Kommentar Bundesverfassung, Bâle 2015.

Zuiderveen Borgesius Frederik, Discrimination, artificial intelligence and algorithmic decision-making, Strasbourg 2018.

Documentation

BFEH, Guide Communication numérique accessible, Version 2.0, 2018.

BFEH, Fiche d'information Langue facile à lire, Version 2.1, 2019.

Bundestag allemand, Menschenrechte im digitalen Zeitalter, WD2-3000-107/18, 3.8.2018.

CDIP, Mesures relatives à la stratégie numérique de la CDIP, 27.6.2019.

Centrale de compensation, Statut dans le domaine de l'AVS/AI/APG au regard du droit des assurances sociales, Mémento, 2017.

Comité des droits de l'enfant, The Committee on the Rights of the Child warns of the grave physical, emotional and psychological effect of the COVID-19 pandemic on children and calls on States to protect the rights of children, 8.4.2020.

Comité des droits de l'enfant, Observation générale No 25, Children's rights in relation to the digital environment, 2.3.2021.

Comité des droits économiques, sociaux et culturels, Observation générale n° 25 (2020) sur la science et les droits économiques, sociaux et culturels, E/C.12/GC/25, 30.4.2020.

Comité des Ministres du Conseil de l'Europe, Recommandation N° R (97) 20 sur le discours de haine, 30.10.1997.

Commission européenne, L'intelligence artificielle pour l'Europe, Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions, COM 237/2018, 25.4.2018.

Conseil des États, Postulat 16.4169, Environnement de travail inclusif à l'ère de la numérisation, 16.12.2016.

Conseil fédéral, Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 15.9.2017.

Conseil fédéral, La gestion des menaces, en particulier dans le contexte de la violence domestique, Rapport du Conseil fédéral en exécution du postulat Feri 13.3441, 11.10.2017.

Conseil fédéral, Conséquences de la numérisation sur l'emploi et les conditions de travail : opportunités et risques, Rapport du Conseil fédéral donnant suite aux postulats 15.3854 Reynard du 16 septembre 2015 et 17.3222 Derder, 8.11.2017.

Conseil fédéral, Commerce de l'or produit en violation des droits humains, Rapport du Conseil fédéral donnant suite au postulat 15.3877, Recordon, 14.11.2018.

Conseil fédéral, Technologies civiques et simplification de la procédure de consultation : développements et mesures, Rapport du Conseil fédéral en exécution des postulats 17.3149 Markus Hausammann et 17.4017 Damian Müller, 8.5.2020.

Conseil fédéral, Stratégie Suisse numérique, 2020.

Conseil national, Interpellation 18.3282, Empêcher les atteintes au principe de solidarité dans l'assurance de base, 18.3.2018.

FNS, Règlement relatif à l'encouragement des publications en libre accès (Open-Access), 7.11.2017.

Gemeinderat Stadt Bern, Online-Angebote, Effort für mehr Barrierefreiheit, communiqué de presse, 16.8.2018.

Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, Polizei Hamburg löscht die im Zuge der G20-Ermittlungen erstellte biometrische Datenbank zum Gesichtsabgleich, 28.5.2020.

Haut-Commissariat des Nations Unies aux droits de l'homme, Human Rights in a New Era, Speech at the University of Geneva by UN High Commissioner for Human Rights Michelle Bachelet, 14.11.2018, disponible sur : <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23874&LangID=E> (consulté en dernier le 30 décembre 2020).

Haut-Commissariat des Nations Unies aux droits de l'homme, Question de la réalisation des droits économiques, sociaux et culturels dans tous les pays, rôle des nouvelles technologies pour la réalisation des droits économiques, sociaux et culturels, A/HRC/43/29, 4.3.2020.

Haut-Commissariat des Nations Unies aux droits de l'homme, Incidence des nouvelles technologies sur la promotion et la protection des droits de l'homme dans le contexte des rassemblements, y compris des manifestations pacifiques, A/HRC/44/24, 24.6.2020.

OCDE, Is there a role for blockchain in responsible supply chains ?, 11.9.2019.

OCDE, Going Digital, Shaping Policies, Improving Lives, résumé en français Vers le numérique : Forger des politiques au service de vies meilleures, 11.3.2019.

OFCOM, Défense contre les violations des droits (de la personnalité) commises par des tiers sur les réseaux sociaux : moyens à la disposition des particuliers, 2013.

PFPDT, Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée), 2013.

PFPDT, Explications concernant le webtracking, 2014, disponible sur : <https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/explications-concernant-le-webtracking.html> (consulté en dernier le 30 décembre 2020).

PFPDT/Privatim, Leitfaden der Datenschutzbehörden von Bund und Kantonen zur Anwendung des Datenschutzrechts auf die digitale Bearbeitung von Personendaten im Zusammenhang mit Wahlen und Abstimmungen in der Schweiz, 2019.

PFPDT, Explications concernant l'informatique en nuage (cloud computing), sans date, disponible sur : <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing.html> (consulté en dernier le 30 décembre 2020).

Point de contact britannique pour les principes directeurs de l'OCDE à l'intention des entreprises, Privacy International & Gamma International UK Ltd, Final Statement, 2014.

Prévention CH, Cyberharcèlement, Agir de bon droit, 2e édition, 2017.

Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, Rapport annuel, A/HRC/34/61, 21.2.2017.

Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Surveillance et droits de l'homme, A/HRC/41/35, 28.5.2019.

Rapporteur spécial sur le droit à l'éducation, Droit à l'éducation à l'ère numérique, A/HRC/32/37, 6.4.2016.

Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté, État-providence numérique, A/74/48037, 11.10.2019.

Regierungsrat Kanton Zürich, Impulsprogramm Digitale Verwaltung 2020, 1.4.2020.

SECO, Commentaire des ordonnances 3 et 4 relatives à la loi sur le travail, Protection de la santé, Approbation des plans, 2020.

SEFRI, Défis de l'intelligence artificielle, Rapport du groupe de travail interdépartemental « Intelligence artificielle » au Conseil fédéral, 13.12.2019.

Auteures

Sabrina Ghielmini

Master en droit, avocate, collaboratrice scientifique auprès du Centre de compétence pour les droits humains (MRZ) de l'Université de Zurich et auprès du domaine thématique Droits humains et économie du CSDH.

Christine Kaufmann

Docteure en droit, professeure ordinaire de droit public, de droit international et de droit européen, présidente du Comité directeur du Centre de compétence pour les droits humains (MRZ) de l'Université de Zurich et responsable du domaine thématique Droits humains et économie du CSDH.

Charlotte Post

Master en droit, collaboratrice auprès du domaine thématique Droits humains et économie du CSDH.

Tina Büchler

Docteure en sciences naturelles, collaboratrice auprès du Centre interdisciplinaire pour la recherche en études genre (IZFG) de l'Université de Berne et auprès du domaine thématique Politique genre du CSDH.

Mara Wehrli

Assistante auxiliaire auprès du Centre interdisciplinaire pour la recherche en études genre (IZFG) de l'Université de Berne, domaine Postcolonialisme.

Michèle Amacker

Docteure en sociologie, professeure assistante pour la recherche en études genre, coresponsable du Centre interdisciplinaire pour la recherche en études genre (IZFG) de l'Université de Berne et responsable du domaine thématique Politique genre du CSDH.

La numérisation peut devenir une précieuse alliée des droits fondamentaux et des droits humains dans les domaines les plus divers, mais les technologies numériques sont aussi susceptibles d'aggraver les violations de ces droits et d'en faire émerger de nouvelles.
Le présent guide, publié par le Centre suisse de compétence pour les droits humains (CSDH), fait un tour d'horizon des effets au quotidien de la numérisation sur les droits fondamentaux et les droits humains. Dans la première partie, les auteures présentent les principales technologies et leurs applications ainsi que les bases légales en la matière. Dans la seconde, elles expliquent, à l'aide de cas concrets, en quoi les droits fondamentaux et les droits humains sont touchés par l'évolution et les applications des technologies numériques. Un ouvrage qui vient nourrir le débat sur la manière de concilier la numérisation et nos droits.

Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Centre suisse de compétence pour les droits humains (CSDH)
Centro svizzero di competenza per i diritti umani (CSDU)
Swiss Centre of Expertise in Human Rights (SCHR)

buch & netz