

# Visages en jeu, ou enjeux de la reconnaissance faciale

## Une analyse à travers le prisme des droits fondamentaux et du droit de la protection des données

FLAMINIA DAHINDEN\*

MOTS CLEFS	protection des données – reconnaissance faciale – droits fondamentaux – données biométriques
ZUSAMMENFASSUNG	Aufgrund ihrer Funktionsweise und ihrer möglichen (oder potenziellen) Anwendungen berührt die Gesichtserkennung die Grundrechte und den Schutz der Persönlichkeit. Dieser Beitrag befasst sich mit dem Schweizer Rechtssystem, das auf diese Technologie anwendbar ist, und den sich daraus ergebenden Verpflichtungen, insbesondere für öffentliche Behörden. Obwohl das Datenschutzrecht allgemeine und spezifische «technisch neutrale» Grundsätze aufstellt, werden diese angesichts der Verwendung von Gesichtserkennungssoftware teilweise untergraben. In bestimmten Konstellationen wäre ein spezifischerer Rahmen wünschenswert, sowohl im privaten als auch im öffentlichen Sektor.
RÉSUMÉ	En raison de son fonctionnement et de ses possibles (ou potentielles) applications, la reconnaissance faciale touche aux droits fondamentaux et à la protection de la personnalité. Cette contribution s'intéresse au régime juridique suisse applicable à cette technologie ainsi qu'aux obligations qui en découlent, en particulier pour les autorités publiques. Si le droit de la protection des données instaure des principes généraux et spécifiques « techniquement neutres », ces derniers sont parfois mis à mal face aux logiciels de reconnaissance faciale. Un encadrement plus spécifique serait souhaitable dans certaines constellations, tant au niveau du secteur privé que public.
ABSTRACT	Because of the way it operates and its possible (or potential) applications, facial recognition affects fundamental rights and the protection of privacy. This contribution focuses on the Swiss legal regime applicable to this technology and the obligations arising from it, particularly for public authorities. While data protection law establishes general and specific 'technically neutral' principles, these are sometimes undermined by facial recognition software. A more specific framework would be desirable in certain constellations, in both the private and public sectors.

### I. Introduction

Que ce soit pour le déverrouillage des smartphones, l'analyse des habitudes de consommation ou encore les contrôles aux frontières, la reconnaissance faciale automatisée s'est établie dans de nombreux domaines, relevant tant de la sphère privée que de la sphère publique<sup>1</sup>. Le recours à cette technologie par certaines institutions a pu faire couler beaucoup d'encre. Parfois utilisée à l'insu des personnes concernées, ou simplement difficilement re-

connaissable, son utilisation soulève des questions d'ordre sociétal, éthique et juridique. Cette contribution se penche sur ce dernier aspect, à savoir les enjeux juridiques de l'application de la reconnaissance faciale en Suisse, en particulier par les autorités publiques. Avant de s'intéresser au cadre juridique applicable, quelques aspects généraux de la reconnaissance faciale seront présentés (II.). L'analyse portera ensuite sur le régime des droits fondamentaux (III.), puis sur celui du droit de la protection des données (IV.), afin de déterminer si, et à quelles conditions, il peut être fait usage de la technologie de reconnaissance faciale en respectant le cadre légal donné.

\* FLAMINIA DAHINDEN, MLaw, Doctorante et assistante diplômée à l'Université de Fribourg. L'autrice remercie la Prof. Astrid Epiney ainsi que les deux expert.e.s anonymes pour leurs lectures attentives et précieux commentaires. Cette contribution est publiée sous une licence Creative Commons. DOI de cet article: 10.3256/978-3-03929-084-0\_03.

<sup>1</sup> RAJA CHATILA et al., Pourquoi la reconnaissance faciale, posturale et comportementale soulève-t-elle des questionnements éthiques ?, in : Éric Germain/Claude Kirchner/Catherine Tessier (éd.), Pour une éthique du numérique, Paris 2022, 209 ss.

### II. Généralités

#### A. Notions, fonctions et fonctionnement

La reconnaissance faciale (ci-après : RF) appartient aux systèmes dits biométriques qui permettent de procéder à la reconnaissance – automatisée ou humaine – des individus à partir de leurs caractéristiques physiologiques

ou comportementales<sup>2</sup>. Ces dernières concernent, par exemple, les empreintes digitales, l'ADN, l'iris, les traits du visage ou encore la signature, la voix ou la démarche<sup>3</sup>. Les caractéristiques biométriques sont généralement uniques (dans la mesure où elles sont propres à chaque individu)<sup>4</sup>, universelles (car en principe présentes chez toute personne) et permanentes (vu qu'elles sont conservées la vie durant, sous réserve d'une altération naturelle, accidentelle ou volontaire)<sup>5</sup>.

*Nous distinguons ici la reconnaissance faciale au sens strict de la reconnaissance faciale au sens large. La première couvre les systèmes permettant l'authentification, respectivement l'identification, d'un individu alors que la seconde détecte « simplement » les visages et/ou détermine les caractéristiques (âge, genre, origine ethnique, etc.), les traits de personnalité (p. ex. extravertie ou introvertie), ou encore les émotions d'une personne – sans pour autant chercher à l'identifier<sup>6</sup>. Cette distinction nous paraît pertinente dans la mesure où la RF au sens large ne couvre pas des systèmes biométriques (le critère de l'identification univoque faisant défaut). Lorsque le type de RF ne sera pas précisé, les considérations concerneront la RF au sens strict.*

En soi, la RF consiste simplement à associer un visage à une personne donnée, ce qui peut être effectué par des êtres humains (méthodes manuelles) ou des algorithmes (systèmes automatiques)<sup>7</sup>. Les méthodes manuelles sont

généralement utilisées lorsqu'il y a peu d'images faciales à analyser (p. ex. un contrôle d'identité de la police qui consiste en la simple comparaison d'une personne avec un document d'identité)<sup>8</sup>. Les systèmes automatiques, quant à eux, sont développés sur la base de différents modèles algorithmiques (*rule-based* ou *machine learning*, plus spécifiquement *deep learning*)<sup>9</sup> et permettent d'identifier automatiquement des visages dans des images ou des vidéos<sup>10</sup>. Ces systèmes peuvent surpasser les compétences de la reconnaissance humaine<sup>11</sup> et soulèvent diverses problématiques – tant par leur fonctionnement que leur application – dont il sera question dans la présente contribution. Par conséquent, le terme de RF sera utilisé dans ce contexte comme une technologie utilisant des algorithmes d'intelligence artificielle (ci-après : IA) qui permettent, à partir des traits du visage, d'authentifier une personne ou de l'identifier<sup>12</sup>, que ce soit *a posteriori* ou en temps réel<sup>13</sup>.

- L'authentification consiste en la vérification qu'une personne est bien celle qu'elle prétend être<sup>14</sup>. Dans ces cas-là, le logiciel compare un gabarit préenregistré (donnée de référence) avec un seul visage, afin de vérifier si cette personne est la même (comparaison de deux gabarits, dite « 1-v-1 »)<sup>15</sup>.
- L'identification, quant à elle, sert à retrouver une personne au sein d'un groupe d'individus, que ce soit dans un lieu défini, dans une image ou encore dans une base de données<sup>16</sup>. Afin de déterminer qui est la personne X., le logiciel génère un gabarit pour chaque visage testé et vérifie si celui-ci correspond à une personne connue du système (comparaison d'un gabarit avec une base de données de gabarits, dite « 1-v-N »)<sup>17</sup>.

<sup>2</sup> PHILIPPE MEIER, Protection des données – Fondements, principes généraux et droit privé, Berne 2011, N 2244 ; Préposé fédéral à la protection des données et à la transparence (FPFDT), Guide relatif aux systèmes de reconnaissance biométrique, Berne 2009, 5.

<sup>3</sup> FPFDT (n. 2), 5. Pour plus de détails sur les données biométriques, voir : DOMINIKA BLONSKI, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, thèse Berne 2015, 5 ss.

<sup>4</sup> Exception faite pour l'ADN des jumeaux monozygotes, cf. BLONSKI, Biometrische Daten (n. 3), 6.

<sup>5</sup> Par exemple, l'altération des traits du visage par une intervention chirurgicale, cf. BLONSKI, Biometrische Daten (n. 3), 7 ; MEIER (n. 2), N 2246.

<sup>6</sup> Dans le même sens, voir : Commission de l'éthique en science et en technologie (CEST), Les enjeux éthiques soulevés par la reconnaissance faciale, Québec 2020, 9 (disponible sous : <https://www.ethique.gouv.qc.ca/fr/publications/reconnaissance-faciale/>) ; Commission nationale de l'informatique et des libertés (CNIL), Reconnaissance faciale – Pour un débat à la hauteur des enjeux, 15 novembre 2019, 4 (disponible sous : <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux>).

<sup>7</sup> MAËLIG JACQUET/LIONEL GROSSRIEDER, Enjeux et perspectives de la reconnaissance faciale en sciences criminelles, Cri-

minologie 2021, 135 ss, 141 ; STAN Z. LI/ANIL K. JAIN, Introduction, in : Stan Z. Li/Anil K. Jain (éd.), Handbook of Face Recognition, Londres 2011, 1 ss, 1 ; MONIKA SIMMLER/GIULIA CANOVA, Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand, S&D 2023, 105 ss, 107.

<sup>8</sup> Pour plus de détails sur les méthodes d'analyse pour la comparaison manuelle de visages par des expertes, voir : JACQUET/GROSSRIEDER (n. 7), 141 s.

<sup>9</sup> Pour plus de détails sur les différents modèles d'intelligence artificielle, voir : K.R. CHOWDHARY, Fundamentals of Artificial Intelligence, New Delhi 2020.

<sup>10</sup> JACQUET/GROSSRIEDER (n. 7), 142 s. ; SIMMLER/CANOVA, Gesichtserkennungstechnologie (n. 7), 107 s.

<sup>11</sup> LI/JAIN (n. 7), 2.

<sup>12</sup> CEST (n. 6), 9 ; CNIL (n. 6), 3.

<sup>13</sup> NADJA BRAUN BINDER/ELIANE KUNZ/LILIANE OBRECHT, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, 53 ss, N 10 ss. Voir également : III.B.1.

<sup>14</sup> CNIL (n. 6), 3.

<sup>15</sup> CNIL (n. 6), 3 ; JACQUET/GROSSRIEDER (n. 7), 140.

<sup>16</sup> CNIL (n. 6), 3.

<sup>17</sup> CNIL (n. 6), 3 ; JACQUET/GROSSRIEDER (n. 7), 140.

De manière très sommaire, le fonctionnement technique de la RF peut être résumé de la façon suivante : à partir de données d'entrée (p. ex. des images ou des vidéos issues de bases de données), des algorithmes détectent le visage humain, en recensent les caractéristiques<sup>18</sup> pour créer une sorte de modèle de visage – nommé « gabarit » –, puis comparent ce dernier à d'autres modèles déjà collectés ou recensés en direct (données de référence)<sup>19</sup>. La RF étant une technique probabiliste, le résultat de la comparaison représente un pourcentage de correspondance et dépend, par ailleurs, de la fonction que doit remplir la RF dans le cas d'espèce (authentification ou identification)<sup>20</sup>. La probabilité que la personne soit bien celle qui doit être authentifiée ou identifiée est déduite de la comparaison entre les gabarits<sup>21</sup>. Si cette probabilité dépasse un certain seuil déterminé, le système considère qu'il y a correspondance<sup>22</sup>.

Comme tout système probabiliste, le résultat comporte nécessairement un taux d'erreur, appelé « faux positif » lorsqu'une concordance est reconnue à tort ou « faux négatif » lorsqu'une concordance est exclue à tort<sup>23</sup>. Toutefois, selon l'objectif de la RF, le système peut être calibré de façon à diminuer le taux de faux négatifs ou de faux positifs<sup>24</sup>.

## B. Domaines d'application

Au vu des différentes fonctionnalités de la RF, il n'est pas étonnant que cette technologie soit utilisée dans de nombreux domaines<sup>25</sup>. Dans le secteur privé, la RF au sens

large est notamment appliquée à des fins de marketing ou de publicité, dans la mesure où les logiciels de RF permettent l'observation des comportements de consommation de la clientèle (comme le parcours dans les rayons ou encore les expressions faciales face aux produits)<sup>26</sup>. Le déverrouillage des smartphones par un mécanisme d'authentification est un exemple de RF au sens strict. Intégrée par défaut au téléphone, cette fonctionnalité biométrique est utilisée par de nombreuses entreprises fournissant des applications ou des services en ligne (p. ex. pour l'authentification avant un paiement)<sup>27</sup>. Il est également imaginable de recourir à la RF lors de manifestations sportives, afin de s'assurer qu'aucune personne non autorisée ne puisse accéder au stade (identification)<sup>28</sup>.

*En Suisse, un projet des CFF avait alerté la population en avril 2023<sup>29</sup>. En effet, la RF permettant le suivi des déplacements<sup>30</sup>, les CFF avaient lancé un appel d'offres pour l'acquisition d'un nouveau système de mesure de l'affluence, afin d'enregistrer les mouvements des personnes et d'en tirer des informations pertinentes pour l'optimisation des gares (en identifiant p. ex. les goulets d'étranglement). L'une des fonctions prévues dans l'appel d'offres devait permettre la segmentation de la clientèle en fonction de l'âge, du sexe ou de la taille (RF au sens large). Suite aux contestations de l'opinion publique, les CFF ont retiré l'appel d'offres pour publier en juin 2023 une version modifiée, cette fois sans l'option de segmentation<sup>31</sup>.*

<sup>18</sup> En règle générale, les distances entre des points définis du visage sont mesurées à cet effet, p. ex. le rapport entre la bouche, le nez et les yeux, cf. SIMMLER/CANOVA, Gesichtserkennungstechnologie (n. 7), 108.

<sup>19</sup> EMMANUELLE GINDRE, Reconnaissance faciale : un mode de preuve 2.0 ?, AJ Pénal 2023, 123 ss, 123. Pour plus de détails sur le fonctionnement de la technologie de reconnaissance faciale, voir : MURAT KARABOGA et al., Automatisierte Erkennung von Stimme, Sprache und Gesicht, Technische, rechtliche und gesellschaftliche Herausforderungen, Zurich 2022, 57 ss ; LI/JAIN (n. 7), 3 s.

<sup>20</sup> GINDRE (n. 19), 123.

<sup>21</sup> CNIL (n. 6), 3.

<sup>22</sup> CNIL (n. 6), 3.

<sup>23</sup> JACQUET/GROSSRIEDER (n. 7), 156 ; NEIL SELWYN et al., Facial Recognition Technology, in : Rita Matulionyte/Monika Zalnierute (éd.), The Cambridge Handbook of Facial Recognition in the Modern State, Cambridge 2024, 11 ss, 19 s.

<sup>24</sup> Les deux sont intrinsèquement liés : si le taux de « faux positifs » diminue, alors le taux de « faux négatifs » augmente et inversement. Par exemple, si l'objectif prioritaire est de s'assurer qu'aucun suspect ne soit écarté à tort (faux négatifs), le fait de réduire le risque de faux négatifs fera augmenter le risque de considérer à tort d'autres personnes (faux positifs), cf. JACQUET/GROSSRIEDER (n. 7), 156 s.

<sup>25</sup> CHATILA et al. (n. 1), 213 ss.

<sup>26</sup> Agence des droits fondamentaux de l'Union européenne (FRA), Technologie de reconnaissance faciale : considérations relatives aux droits fondamentaux dans le contexte de l'application de la loi, Vienne 2022, 2 (disponible sous : <https://fra.europa.eu/fr/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>).

<sup>27</sup> CNIL, <https://www.cnil.fr/fr/biometrie-dans-les-smartphones-des-particuliers-application-du-cadre-de-protection-des-donnees>, consulté le 4 janvier 2025.

<sup>28</sup> FRA (n. 26), 2 ; BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 10 ; Watson, <https://www.watson.ch/sport/fussball/916971444-gesichtserkennung-beim-fc-sion-datenschuetzer-haette-nichts-dagegen>, consulté le 4 janvier 2025.

<sup>29</sup> CFF, <https://news.sbb.ch/fr/article/116081/le-point-sur-le-projet-de-nouveau-systeme-de-mesure-de-l-affluence>, consulté le 4 janvier 2025 ; CFF, <https://news.sbb.ch/fr/medias/article/116274/flux-de-personnes-dans-les-gares-les-cff-se-concentrent-sur-les-fonctions-cles-et-renoncent-a-la-segmentation>, consulté le 4 janvier 2025.

<sup>30</sup> CNIL (n. 6), 5.

<sup>31</sup> CFF, <https://news.sbb.ch/fr/article/116081/le-point-sur-le-projet-de-nouveau-systeme-de-mesure-de-l-affluence>, consulté le 4 janvier 2025 ; CFF, <https://news.sbb.ch/fr/medias/article/116274/flux-de-personnes-dans-les-gares-les-cff-se-concentrent-sur-les-fonctions-cles-et-renoncent-a-la-segmentation>, consulté le 4 janvier 2025.

La RF est également utilisée par les autorités publiques – principalement par les services de sécurité et de police – notamment dans le cadre de contrôles aux frontières, dans les procédures d'enquêtes<sup>32</sup> ainsi que pour la surveillance du respect de règles spécifiques (p. ex. les règles de quarantaine durant la pandémie du COVID-19)<sup>33</sup>.

Sans prétendre être exhaustifs, ces exemples d'applications permettent de souligner l'importance de cette technologie en pratique, et, par conséquent, celle de sa compatibilité avec les droits fondamentaux et le droit de la protection des données.

### III. Sous l'angle des droits fondamentaux

Au vu de son fonctionnement et de ses possibles applications, la RF touche au domaine de protection de plusieurs droits fondamentaux. Il s'agira, dans un premier temps, de déterminer les droits fondamentaux pouvant être atteints (III.A.) puis, dans un second temps, d'analyser à quelles conditions et dans quelle mesure ces droits peuvent être restreints (III.B.).

#### A. Droits fondamentaux concernés

Il y a atteinte à un droit fondamental lorsqu'un acte de l'État, ou imputable à l'État, affecte le domaine de protection d'un droit fondamental, que ce soit de manière compatible (restriction) ou incompatible (violation) avec la garantie que le droit constitutionnel ou conventionnel accorde à ce droit fondamental<sup>34</sup>. Dans le contexte de cette contribution, l'acte étatique correspond à l'utilisation de la RF.

Lorsque les autorités recourent à des technologies de RF, une atteinte est portée au droit à la protection de la sphère privée (art. 13 al. 1 Cst. ; art. 8 CEDH) ainsi qu'au droit à l'autodétermination informationnelle, respectivement au droit d'être protégé contre l'emploi abusif de données personnelles (art. 13 al. 2 Cst.)<sup>35</sup>.

La protection de la sphère privée, définie comme « droit à l'autodétermination sociale d'une personne physique ou

morale »<sup>36</sup>, permet notamment aux personnes d'établir et d'entretenir des relations sociales sans que les actes ou propos tenus en public ne soient observés ou documentés en permanence par des tiers, en l'occurrence par l'État<sup>37</sup>. En effet, la protection de la sphère privée ne se limite pas au domaine privé, mais s'étend également au domaine public, couvrant ainsi les événements à caractère personnel qui se déroulent dans l'espace public<sup>38</sup>. Si la « simple » vidéosurveillance de l'espace public est déjà considérée par le Tribunal fédéral comme une restriction de la liberté personnelle<sup>39</sup>, le traitement d'images faciales constitue également, *a fortiori*, une ingérence de l'État dans la sphère privée, la confiance en un large anonymat dans l'espace public étant ébranlée<sup>40</sup>.

Le droit à l'autodétermination informationnelle, quant à lui, garantit qu'en principe, toute personne doit pouvoir déterminer, si et dans quel but des informations la concernant peuvent être traitées par des tiers, publics ou privés<sup>41</sup>. Son contenu est concrétisé par le droit de la protection des données<sup>42</sup>, qui sera abordé plus amplement dans le prochain chapitre (IV.).

Par ailleurs, les libertés de la communication, en particulier les libertés d'opinion et d'information (art. 16 Cst. ; art. 10 CEDH), la liberté de réunion ainsi que la liberté d'association (art. 22 et 23 Cst. ; art. 11 CEDH) sont sujettes à des atteintes indirectes<sup>43</sup>. En effet, en plus des atteintes dites directes, un acte étatique peut affecter un droit fondamental, sans que les titulaires de celui-ci ne soit expressément visé.s par cet acte (atteintes indirectes)<sup>44</sup>. Cela peut se produire dans de nombreuses circonstances, notamment lorsque l'acte de l'État en question exerce un effet dissuasif sur les titulaires d'un droit fondamental, si bien que ces dernier.ère.s préfèrent s'abstenir d'exercer ce droit (*chilling effect*)<sup>45</sup>. Dans le contexte de la RF, la possible utilisation d'une telle technologie pour traiter des images capturées par des caméras dans l'espace public peut avoir un effet dissuasif<sup>46</sup>. En effet, elle pourrait décourager certaines personnes d'exercer leur liberté d'expression, de réunion ou d'association – dont l'anonymat

<sup>32</sup> Par exemple, la RF est utilisée pour retrouver des enfants kidnappés, appréhender des personnes recherchées ou encore identifier des victimes ou des personnes dont les documents ont été perdus, cf. KARABOGA et al. (n. 19), 108 ; SELWYN et al. (n. 23), 18 s.

<sup>33</sup> FRA (n. 26), 2 ; BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 14 s. ; SELWYN et al. (n. 23), 18 s.

<sup>34</sup> JACQUES DUBÉY, Droits fondamentaux, Bâle 2018, N 380 ss.

<sup>35</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 26.

<sup>36</sup> DUBÉY (n. 34), N 1774 avec références jurisprudentielles citées.

<sup>37</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 26 ; DUBÉY (n. 34), N 1777.

<sup>38</sup> ATF 146 I 11, 13, c. 3.1.1 ; ATF 118 IV 41, 45, c. 4.

<sup>39</sup> ATF 136 I 87, 112, c. 8.1.

<sup>40</sup> KARABOGA et al. (n. 19), 124.

<sup>41</sup> ATF 146 I 11, 13, c. 3.1.1 ; ATF 145 IV 42, 46 c. 4.2 ; ATF 144 I 281, 301, c. 6.2.

<sup>42</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 27.

<sup>43</sup> KARABOGA et al. (n. 19), 124.

<sup>44</sup> DUBÉY (n. 34), N 416 s.

<sup>45</sup> DUBÉY (n. 34), N 417 ss.

<sup>46</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 30.

est une composante importante<sup>47</sup> – ou les inciter à modifier leur comportement<sup>48</sup>.

De plus, l'utilisation de la technologie de RF peut porter atteinte à l'interdiction de discrimination (art. 8 al. 2 Cst. ; art. 14 CEDH)<sup>49</sup>. En effet, comme explicité ci-dessus (II.A.), le résultat de la RF peut comporter des « faux positifs » ou des « faux négatifs »<sup>50</sup>. La précision<sup>51</sup> – et donc la fiabilité – des logiciels de RF dépendent entre autres des bases de données avec lesquelles ils sont entraînés<sup>52</sup>. Celles-ci devraient être alimentées par de nombreuses images faciales (quantité) représentant différents groupes de personnes (qualité)<sup>53</sup>. Il a néanmoins été constaté que les hommes blancs sont généralement sur-représentés dans les images faciales utilisées pour développer les algorithmes<sup>54</sup>. Les systèmes de RF ont ainsi donné de moins bons résultats pour les personnes non blanches, les femmes, les enfants et les personnes âgées<sup>55</sup>. Par conséquent, l'utilisation de la RF, notamment par la police dans le cadre d'enquêtes criminelles, peut augmenter la probabilité que des personnes racisées soient identifiées à tort et poursuivies pour des délits qu'elles n'ont pas commis<sup>56</sup>. À noter que les algorithmes, dont la programmation est réalisée par des êtres humains, comportent des biais supplémentaires<sup>57</sup>. En effet, la façon dont ils ont été conçus – entre autres par des décisions discrétionnaires et des jugements subjectifs – se reflète dans leurs résultats<sup>58</sup>. Ainsi, il s'agit non seulement de diversifier la base de données,

mais également les équipes de recherche et de développement de ces technologies d'IA<sup>59</sup>.

Finalement, les droits fondamentaux de procédure (art. 29, 29a et 30 Cst. ; art. 6 CEDH) sont également pertinents dans ce contexte. En effet, ils garantissent un droit au recours juridictionnel effectif, aussi à l'encontre de mesures fondées – ou qui sont soupçonnées d'être fondées – exclusivement ou de manière significative sur les résultats d'un système de RF<sup>60</sup>. Il en ressort que la personne concernée devrait être informée du traitement de son image faciale – selon les circonstances, dès que cette information n'est plus susceptible de compromettre une éventuelle enquête<sup>61</sup>.

## B. Conditions de restriction

Afin de déterminer si l'atteinte due à l'utilisation de la RF est compatible avec la garantie des droits fondamentaux cités ci-dessus, il y a lieu de procéder au traditionnel examen des conditions de restriction consacrées à l'art. 36 Cst., à savoir s'il existe une base légale suffisante (al. 1), si la restriction du droit fondamental concerné est justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui (al. 2) et, finalement, si l'utilisation de la RF est une mesure proportionnée par rapport au but visé (al. 3). Le régime de restriction de la CEDH est similaire à celui prévu par la Constitution fédérale<sup>62</sup>.

### 1. Base légale

Selon l'art. 36 al. 1 1<sup>re</sup> phrase Cst., « [t]oute restriction d'un droit fondamental doit être fondée sur une base légale ». L'exigence de formalité de la base légale, ainsi que de sa densité normative, se fait en fonction de l'intensité de l'atteinte : plus l'intensité de la restriction est haute, plus le rang hiérarchique et la précision de la base légale doivent

<sup>47</sup> MONIKA ZALNIERIUTE, Power and Protest, Facial Recognition and Public Space Surveillance, in : Rita Matulionyte/Monika Zalnierute (éd.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge 2024, 96 ss, 102 ss.

<sup>48</sup> FRA (n. 26), 33.

<sup>49</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 31 s.

<sup>50</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 31 ; JACQUET/GROSSRIEDER (n. 7), 156.

<sup>51</sup> Par précision, il faut entendre la probabilité que deux images représentent effectivement la même personne lorsque le logiciel indique un résultat positif, cf. JACQUET/GROSSRIEDER (n. 7), 157.

<sup>52</sup> FRA (n. 26), 31 ; JACQUET/GROSSRIEDER (n. 7), 155 ; JASCHA KOLBERG et al., On the Potential of Algorithm Fusion for Demographic Bias Mitigation in Face Recognition, *IET Biometrics* 2024, 1808587.

<sup>53</sup> Pour plus de détails, voir : FRA (n. 26), 31.

<sup>54</sup> FRA (n. 26), 31 ; JACQUET/GROSSRIEDER (n. 7), 155.

<sup>55</sup> CEST (n. 6), 18 ; KARABOGA et al. (n. 19), 123.

<sup>56</sup> MARCUS SMITH/MONIQUE MANN, Facial Recognition Technology and Potential for Bias and Discrimination, in : Rita Matulionyte/Monika Zalnierute (éd.), *The Cambridge Handbook of Facial Recognition in the Modern State*, Cambridge 2024, 87 ss, 89 ss ; FRA (n. 26), 31 s.

<sup>57</sup> CEST (n. 6), 18.

<sup>58</sup> SELWYN et al. (n. 23), 22.

<sup>59</sup> SELWYN et al. (n. 23), 22.

<sup>60</sup> FRA (n. 26), 35 s. ; Conseil de l'Europe, *Décoder l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme*, Strasbourg 2019, 14 s. (disponible sous : <https://rm.coe.int/decoder-l-intelligence-artificielle-10-mesures-pour-protoger-les-droit/168094b6e2>).

<sup>61</sup> KARABOGA et al. (n. 19), 124. Pour plus de détails, également concernant la jurisprudence de la CJUE, voir : FRA (n. 26), 35 s.

<sup>62</sup> L'ingérence doit être prévue par la loi, constituer une mesure nécessaire dans une société démocratique et poursuivre des buts d'intérêt public. À noter que les conditions de restriction ne se trouvent pas, à l'instar de l'art. 36 Cst., dans une clause générale, mais figurent le cas échéant sous chaque garantie (p.ex. art. 8 par. 2, art. 10 par. 2 et art. 11 par. 2 CEDH), cf. DUBÉY (n. 34), N 490 ss.

être élevés<sup>63</sup>. L'appréciation de l'intensité de l'atteinte, respectivement la distinction entre restriction simple et restriction grave, ne repose pas sur un critère précis mais dépend bien plus des circonstances du cas d'espèce<sup>64</sup>.

Dans le cadre de la RF, plusieurs critères peuvent aider à évaluer la gravité d'une atteinte aux droits fondamentaux, tels que la nature du traitement, son ampleur temporelle et spatiale, ou encore la catégorie de données concernées<sup>65</sup>.

Ainsi, la fonctionnalité que remplit la RF dans le cas d'espèce joue un certain rôle – l'atteinte étant par exemple plus faible pour une authentification, qui se limite à la comparaison de deux images faciales (« 1-v-1 »), que pour une identification, qui constitue un traitement (de masse) automatisé et systématique avec davantage de possibilités de surveillance (« 1-v-N »)<sup>66</sup>.

Le laps de temps qui s'écoule entre l'acquisition des données biométriques et son traitement est également un élément important à prendre en compte. L'identification biométrique à distance peut se faire en temps réel ou *a posteriori*<sup>67</sup>. Dans le premier cas de figure, l'identification se fait instantanément (ou avec un léger décalage temporel), alors que dans le second cas de figure, les données biométriques sont d'abord collectées, et la comparaison ainsi que l'identification n'ont lieu qu'ultérieurement<sup>68</sup>.

L'utilisation de systèmes de RF en temps réel présente des risques accrus pour les libertés et les droits fondamentaux des individus. Elle peut notamment engendrer un sentiment de surveillance constante, dissuader l'exercice de la liberté de réunion et présenter des imprécisions techniques pouvant conduire à des discriminations, en particulier lorsqu'elle est utilisée à des fins répressives<sup>69</sup>.

*La CourEDH s'est exprimée dans l'affaire Glukhin c. Russie au sujet de l'atteinte causée par l'utilisation des méthodes de reconnaissance biométrique en temps réel<sup>70</sup>. Elle a estimé que le recours à la RF « à la volée » était une mesure particulièrement intrusive et que, par conséquent, le niveau de justification le plus élevé était requis pour l'utilisation de cette technologie<sup>71</sup>. Ainsi, une RF en temps réel doit être considérée comme une atteinte grave à l'art. 8 CEDH, respectivement l'art. 13 al. 2 Cst.*

*Contrairement à d'autres pays, les autorités suisses ne font pas (ou du moins pas encore) usage de systèmes de RF en temps réel<sup>72</sup>.*

Par ailleurs, le traitement des données qualifiées de sensibles au sens de la LPD<sup>73</sup> peut être un indice d'atteinte grave<sup>74</sup>. En effet, la RF génère et traite des informations biométriques qui bénéficient d'une protection particulière<sup>75</sup>, ce qui plaide en faveur d'une qualification d'atteinte grave au droit à la protection de la sphère privée (art. 13 al. 1 Cst.)<sup>76</sup>.

*Dans l'ATF 149 I 218, le Tribunal fédéral a estimé que la recherche automatique de véhicules constituait une atteinte grave au droit à l'autodétermination en matière d'informations personnelles<sup>77</sup>. Il a précisé – bien que seules les plaques minéralogiques aient été photographiées automatiquement dans le cas d'espèce – que si les personnes occupant le véhicule devaient également être photographiées, une base légale formelle spécifique à ce sujet serait requise, car il s'agirait d'une atteinte grave<sup>78</sup>.*

<sup>63</sup> EVA MARIA BELSER, Der grundrechtliche Rahmen des Datenschutzes, in : Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (éd.), Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011, 319 ss, N 125 ; DUBEY (n. 34), N 428.

<sup>64</sup> DUBEY (n. 34), N 428 ss.

<sup>65</sup> MONIKA SIMMLER/GIULIA CANOVA, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren – Ein weiterer Beitrag zu einer anhaltenden Debatte, RDS 2023, 201 ss, 207.

<sup>66</sup> SELWYN et al. (n. 23), 11 s.

<sup>67</sup> CEST (n. 6), 10. Voir également : art. 3 pt. 42 s. du Règlement (UE) 2024/1689 du 13 juin 2024 sur l'intelligence artificielle (JO L 2024/1689 du 12 juillet 2024).

<sup>68</sup> L'utilisation de systèmes de RF *a posteriori* implique que les images ou vidéos proviennent initialement de caméras de surveillance en circuit fermé et que l'analyse par le logiciels de RF n'intervient que dans un second temps, généralement après une infraction et pendant les poursuites pénales. Dans ce cas d'espèce, l'identification concrète de la personne concernée reste du ressort de l'autorité et non du logiciel, cf. BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 14.

<sup>69</sup> FRA (n. 26), 20 ss ; SIMONE KUHLMANN, Government Use of Facial Recognition – Technologies under European Law, in :

Rita Matulionyte/Monika Zalnieriute (éd.), The Cambridge Handbook of Facial Recognition in the Modern State, Cambridge 2024, 127 ss, 131. Voir également : pt. 32 du préambule du Règlement (UE) 2024/1689 du 13 juin 2024 sur l'intelligence artificielle (JO L 2024/1689 du 12 juillet 2024).

<sup>70</sup> CEDH, *Glukhin c. Russie*, 11519/20 (4 juillet 2023).

<sup>71</sup> CEDH, *Glukhin c. Russie*, 11519/20 (4 juillet 2023), § 86.

<sup>72</sup> KARABOGA et al. (n. 19), 114.

<sup>73</sup> Cf. IV.A.1.

<sup>74</sup> Il est toutefois possible que le traitement de données personnelles sensibles ne constitue pas une atteinte grave au sens de l'art. 36 al. 1 Cst. et, inversement, que le traitement de données personnelles (non qualifiées) porte une atteinte grave à un droit fondamental, cf. BELSER (n. 63), N 128.

<sup>75</sup> BLONSKI, Biometrische Daten (n. 3), 69 ; SIMMLER/CANOVA, Gesichtserkennung im Strafverfahren (n. 65), 207.

<sup>76</sup> SIMMLER/CANOVA, Gesichtserkennung im Strafverfahren (n. 65), 207. Voir également : IV.A.

<sup>77</sup> ATF 149 I 218, 225, c. 8.1.1. Déjà dans le même sens, voir : ATF 146 I 11, 15, c. 3.2.

<sup>78</sup> ATF 149 I 218, 228, c. 8.4.1.

Si les restrictions sont à qualifier de graves, elles doivent être prévues par une loi au sens formel (art. 36 al. 1 2<sup>e</sup> phrase Cst.), c'est-à-dire par un acte adopté par le parlement selon la procédure législative ordinaire<sup>79</sup>. À noter que cette exigence n'exclut pas le recours à la délégation législative. Une clause de délégation législative est en effet possible si elle est contenue dans une loi au sens formel, se limite à une matière ou à un aspect déterminé, contient les grandes lignes des règles de droit à adopter et n'est pas exclue par la Constitution (art. 164 al. 2 i.f. Cst.)<sup>80</sup>. Par conséquent, la loi au sens formel doit au moins prévoir la possibilité d'une utilisation de la RF.

*À titre d'exemple, la loi fédérale sur les étrangers et l'intégration (LEI)<sup>81</sup> prévoit que l'arrivée des passagers à l'aéroport peut être surveillée par des moyens techniques de reconnaissance et qu'il revient au Conseil fédéral de déterminer les spécificités d'un tel système de reconnaissance des visages (art. 103 al. 1 et 5 LEI). Ainsi, l'ordonnance sur l'entrée et l'octroi de visas (OEV)<sup>82</sup> consacre plusieurs dispositions aux conditions générales pour l'admissibilité de l'utilisation d'un système de reconnaissance faciale par les autorités chargées du contrôle à la frontière (art. 54 ss OEV).*

Outre l'exigence de formalité, la base légale doit être suffisamment précise (densité normative)<sup>83</sup>. Le degré de précision requis ne peut être déterminé de manière abstraite, car il dépend, entre autres, de la diversité des situations à réglementer, de la complexité et de la prévisibilité des décisions à prendre dans chaque cas d'espèce, des destinataires de la norme ainsi que de la gravité de l'atteinte aux droits fondamentaux<sup>84</sup>.

Dans le contexte de la RF, la loi devrait notamment indiquer le type de traitement (p. ex. la collecte, l'enregistrement, la conservation, l'évaluation, etc.) ainsi que son étendue (quoi, quand et où), le but concret du traitement, l'utilisation spécifique de la technologie de RF, les catégories de données traitées, les autorités impliquées ou les personnes autorisées à accéder au traitement, la conservation et l'effacement des données, la garantie des droits des personnes concernées, mais aussi la mise en œuvre tech-

nique du système de surveillance (fiabilité et précision de l'algorithme, traçabilité du processus, mesures de sécurité et responsables du système)<sup>85</sup>. Le simple renvoi à un intérêt public, comme la sécurité publique, la protection des personnes ou l'accomplissement des tâches de la police, n'est pas suffisant<sup>86</sup>.

*Il convient de souligner ici qu'une partie de la doctrine considère que les bases légales suisses ne sont pas suffisamment précises pour encadrer l'utilisation de la reconnaissance faciale dans le cadre de la procédure pénale ou du droit cantonal de la police<sup>87</sup>, bien que cette technologie soit déjà utilisée<sup>88</sup>.*

## 2. Intérêt public prépondérant

Un intérêt public est dit prépondérant au sens de l'art. 36 al. 2 Cst. lorsqu'il s'agit d'un intérêt public d'une catégorie suffisamment importante pour qu'il soit susceptible de justifier une restriction à un droit fondamental<sup>89</sup>. Une telle qualification dépend d'un jugement de valeur abstrait porté sur l'importance de l'intérêt public en cause et de l'intérêt privé opposé<sup>90</sup>.

*Dans l'ATF 149 I 218 concernant la recherche automatique de véhicules, le Tribunal fédéral a souligné que la réutilisation et l'échange de données provenant d'une atteinte grave à l'autodétermination en matière d'information devaient viser un intérêt public d'une importance comparable à celui visé lors de la collecte des données<sup>91</sup>. La transmission pour l'accomplissement d'une quelconque tâche de l'autorité requérante ne constituerait donc pas un intérêt suffisant, susceptible de prévaloir lors de la pesée des intérêts<sup>92</sup>.*

La sécurité et l'ordre publics sont généralement pertinents pour justifier une atteinte due à l'utilisation de la

<sup>79</sup> DUBÉY (n. 34), N 558 ss.

<sup>80</sup> DUBÉY (n. 34), N 558 ss et 570 ss.

<sup>81</sup> Loi fédérale du 16 décembre 2005 sur les étrangers et l'intégration (LEI ; RS 142.20).

<sup>82</sup> Ordonnance du 15 août 2018 sur l'entrée et l'octroi de visas (OEV ; RS 142.204).

<sup>83</sup> BELSER (n. 63), N 125.

<sup>84</sup> ATF 135 I 169, 173, c. 4.5.1 ; ATF 131 II 271, 278, c. 6 ; KARABOGA et al. (n. 19), 126.

<sup>85</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 28 ; KARABOGA et al. (n. 19), 126 s.

<sup>86</sup> FRA (n. 26), 23 ; BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 28.

<sup>87</sup> SIMMLER/CANOVA, Gesichtserkennung im Strafverfahren (n. 65), 212 ss. Voir également : BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 29.

<sup>88</sup> RTS, <https://www.rts.ch/info/suisse/13487224-l'utilisation-des-logiciels-de-reconnaissance-faciale-par-la-police-pose-questions.html>, consulté le 20 décembre 2024.

<sup>89</sup> DUBÉY (n. 34), N 709 ss.

<sup>90</sup> DUBÉY (n. 34), N 711.

<sup>91</sup> ATF 149 I 218, 236, c. 8.9.2. Voir également : TF 1C\_63/2023 (17 octobre 2024), c. 6.6.3.

<sup>92</sup> ATF 149 I 218, 236, c. 8.9.2.

RF<sup>93</sup>, dans la mesure où ils peuvent potentiellement prévaloir – lors de la pesée des intérêts – sur les intérêts privés opposés, soit les droits fondamentaux cités ci-dessus (III.A.). Il peut s'agir de la prévention ou de l'élimination d'infractions – notamment en cas d'attaques terroristes ou de délits graves – ou encore de la recherche de personnes disparues<sup>94</sup>. La santé publique constitue également un intérêt public susceptible de justifier une atteinte<sup>95</sup>. À titre d'exemple, certains pays ont fait recours à la RF lors du COVID-19, afin de détecter de potentiels symptômes<sup>96</sup>.

Étant donné que les droits fondamentaux concernés – tels que la protection de la sphère privée et les libertés d'opinion et d'information – sont également d'intérêt public, car essentiels pour le bon fonctionnement d'une démocratie, l'intérêt public opposé doit revêtir une haute importance. *A priori*, un intérêt économique serait insuffisant.

### 3. Proportionnalité

En plus de l'exigence d'une base légale suffisante et d'un intérêt public prépondérant, une restriction à un droit fondamental doit être proportionnée au but visé (art. 36 al. 3 Cst.). La mesure doit être apte à et nécessaire pour atteindre ce but, ainsi que raisonnablement exigible au vu de l'intérêt privé lésé<sup>97</sup>.

La question de l'aptitude est spécialement importante dans le contexte de la RF. En effet, il s'agit d'évaluer si la technologie utilisée est de nature à atteindre l'intérêt visé. En général, l'utilisation des logiciels de RF semble appropriée pour retrouver en particulier des personnes disparues ou des criminels recherchés<sup>98</sup>. Néanmoins, en lien avec les considérations sur les taux d'erreurs et leurs potentielles conséquences (III.A.), un système de RF présentant un taux d'erreur très élevé ne serait pas une mesure apte, vu que les résultats ne seraient pas fiables<sup>99</sup>. De plus, une concordance ne devrait constituer qu'un indice d'enquête et non pas une identification définitive.

Le critère de nécessité, quant à lui, impose de choisir parmi l'ensemble des mesures aptes, celle qui porte le moins atteinte aux intérêts privés opposés<sup>100</sup>. Concrètement, il s'agit de déterminer si la RF constitue le moyen

le moins incisif permettant d'atteindre les buts visés. Dans certaines circonstances, il est possible que l'objectif puisse être atteint sans la reconnaissance faciale – par exemple en faisant appel à des « super-physionomistes »<sup>101</sup>. Si l'utilisation de la RF est nécessaire, il faut choisir les modalités les moins incisives, en limitant notamment le périmètre géographique et la durée du traitement, en choisissant un traitement *a posteriori* plutôt qu'en temps réel, ou en adaptant la conservation des données<sup>102</sup>.

*Dans l'analyse de la proportionnalité, il faut non seulement éviter que des technologies inutilement intrusives soient utilisées, mais également prendre en compte la possible combinaison de différentes technologies qui démultiplie leur impact sur les individus (p. ex. une vidéo-surveillance couplée d'une RF automatisée)*<sup>103</sup>.

Finalement, la proportionnalité au sens strict permet de vérifier le caractère raisonnable du rapport entre but visé et moyen utilisé<sup>104</sup>. La pesée des intérêts se fait en fonction de la situation concrète et de l'utilisation de la RF, la proportionnalité et le but de la technologie étant très imbriqués.

*Dans l'arrêt 1C\_63/2023 du 17 octobre 2024, le Tribunal fédéral a procédé au contrôle abstrait de certaines dispositions de la loi lucernoise sur la police*<sup>105</sup>. *Il a notamment rendu lettre-morte une disposition concernant la recherche automatique de véhicules et la surveillance du trafic en raison de l'atteinte disproportionnée aux droits fondamentaux*<sup>106</sup>. *Elle prévoyait non seulement la photographie des plaques d'immatriculation mais également des personnes occupant le véhicule, permettait la création de profils de déplacement (« profilage ») sans conditions ou garanties procédurales et conservait toutes les données pendant cent jours, y compris en cas de non-concordance*<sup>107</sup>.

<sup>93</sup> BELSER (n. 63), N 136.

<sup>94</sup> KARABOGA et al. (n. 19), 127.

<sup>95</sup> KARABOGA et al. (n. 19), 127.

<sup>96</sup> SELWYN et al. (n. 23), 12.

<sup>97</sup> BELSER (n. 63), N 143 ; KARABOGA et al. (n. 19), 127.

<sup>98</sup> KARABOGA et al. (n. 19), 127.

<sup>99</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 32 ; KARABOGA et al. (n. 19), 127.

<sup>100</sup> DUBEY (n. 34), N 750.

<sup>101</sup> C'est le cas p. ex. des polices cantonale et municipale de Saint-Gall, qui ont recours à des agents super-physionomistes, cf. Le Nouvelliste, <https://www.lenouvelliste.ch/suisse/reconnaissance-faciale-st-gall-innovent-en-misant-sur-des-policiers-super-physionomistes-1407272>, consulté le 22 décembre 2024. Voir également : KARABOGA et al. (n. 19), 128.

<sup>102</sup> KARABOGA et al. (n. 19), 128.

<sup>103</sup> CNIL (n. 6), 4.

<sup>104</sup> DUBEY (n. 34), N 754.

<sup>105</sup> TF 1C\_63/2023 (17 octobre 2024).

<sup>106</sup> TF 1C\_63/2023 (17 octobre 2024), c. 3.6.

<sup>107</sup> TF 1C\_63/2023 (17 octobre 2024), c. 3.6.

#### IV. Sous l'angle du droit de la protection des données

Outre les dispositions constitutionnelles, il convient également de s'intéresser aux dispositions légales pertinentes dans le contexte de la RF, plus particulièrement à la législation sur la protection des données. Dans le contexte de cette contribution, il sera fait référence à la loi fédérale sur la protection des données (LPD)<sup>108</sup> qui s'applique au traitement de données personnelles effectué par des personnes privées ou par des organes fédéraux (art. 2 al. 1 LPD) – les traitements de données effectués par des organes cantonaux étant régis par le droit cantonal<sup>109</sup>. Les considérations du présent chapitre sont toutefois applicables *mutatis mutandis* aux législations cantonales, ces dernières étant largement similaires au droit fédéral en raison de l'obligation de conformité à la Constitution fédérale ainsi qu'au droit international<sup>110</sup>.

Comme énoncé en son article premier, la LPD vise à protéger la personnalité et les droits fondamentaux des personnes physiques dont les données personnelles font l'objet d'un traitement<sup>111</sup>, et non les données en tant que telles<sup>112</sup>. La protection de la personnalité vise en premier lieu les traitements effectués par des personnes privées (physiques ou morales), alors que le respect des droits fondamentaux – comme présenté précédemment (III.) – s'adresse uniquement aux autorités publiques<sup>113</sup>. Dans ce chapitre, il sera d'abord question de la qualification, au sens de la LPD, des données traitées lors de l'utilisation de la technologie de RF et des conséquences qui en découlent (IV.A.). Ensuite, les différents principes généraux

du droit de la protection des données seront mis en lien avec l'utilisation de la RF (IV.B.). Finalement, les différentes conditions de licéité d'un tel traitement de données seront analysées, selon qu'il est réalisé par des personnes privées ou des organes fédéraux (IV.C.).

##### A. Traitement de données personnelles

La notion de « traitement de données personnelles » est centrale, car elle délimite le champ d'application de la LPD (art. 2 al. 1 LPD)<sup>114</sup>. Elle peut brièvement être définie comme toute opération relative à des données personnelles – à savoir toute information, indépendamment de leur forme ou contenu, concernant une personne physique identifiée ou identifiable<sup>115</sup> – quels que soient les moyens et procédés utilisés (cf. art. 5 let. a et d LPD)<sup>116</sup>. La LPD est donc technologiquement neutre et couvre toutes les méthodes de traitement, mêmes celles encore inconnues aujourd'hui<sup>117</sup>.

Étant donné que la RF consiste en un traitement automatique d'images contenant des visages de personnes, entre autres à des fins d'authentification et d'identification<sup>118</sup>, son utilisation par des personnes privées ou des organes fédéraux tombe dans le champ d'application de la LPD.

##### 1. Données personnelles sensibles

La LPD prévoit une sous-catégorie de données personnelles, à savoir les données personnelles sensibles (ci-après : données sensibles), qui bénéficient d'une protection spécifique en raison du risque accru que leur traitement peut entraîner pour la personnalité et les droits fondamentaux de la personne concernée<sup>119</sup>. Les différentes catégories de données sensibles sont listées

<sup>108</sup> Loi fédérale du 25 septembre 2020 sur la protection des données (LPD ; RS 235.1).

<sup>109</sup> DOMINIKA BLONSKI, Was bedeutet die Revision für die kantonalen Datenschutzgesetze?, in : Astrid Epiney/Sophie Moser/Sophia Rovelli (éd.), Die Revision des Datenschutzgesetzes des Bundes/La révision de la Loi fédérale sur la protection des données, Zurich/Bâle/Genève 2022, 89 ss, 92.

<sup>110</sup> BLONSKI, kantonale Datenschutzgesetze (n. 109), 92 ; KARABOGA et al. (n. 19), 129.

<sup>111</sup> La LPD concrétise ainsi non seulement la protection de la sphère privée en tant que droit fondamental (art. 13 Cst.), mais également la protection de la personnalité en droit privé (art. 28 ss CC), cf. SYLVAIN MÉTILLE, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020 : des principes, des droits et des obligations, in : Astrid Epiney/Sophie Moser/Sophia Rovelli (éd.), Die Revision des Datenschutzgesetzes des Bundes/La révision de la Loi fédérale sur la protection des données, Zurich/Bâle/Genève 2022, 1 ss, 5 ; CR LPD-COTTIER, art. 1 N 12 ss.

<sup>112</sup> SANDRA HUSI-STÄMPFLI et al., Protection des données, Zurich/Genève 2024, 38.

<sup>113</sup> HUSI-STÄMPFLI et al. (n. 112), 38.

<sup>114</sup> CR LPD-MEIER/TSCHUMY, art. 5 N 18 et 72.

<sup>115</sup> Une personne est « identifiée » lorsqu'il ressort de l'information même qu'il s'agit précisément de cette personne, alors qu'elle est « identifiable » s'il est possible de déduire son identité par corrélation d'informations tirées des circonstances ou du contexte (comme p. ex. un numéro de téléphone, une adresse ou une date de naissance), cf. Message du 15 septembre 2017 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 (LPD), FF 2017 6565 ss, 6639 ; HUSI-STÄMPFLI et al. (n. 112), 52 ; MÉTILLE (n. 111), 4.

<sup>116</sup> Pour plus de détails sur la délimitation de ces notions, voir : CR LPD-MEIER/TSCHUMY, art. 5 N 18 ss et 72 ss.

<sup>117</sup> HUSI-STÄMPFLI et al. (n. 112), 60.

<sup>118</sup> FRA (n. 26), 7.

<sup>119</sup> BLONSKI (n. 3), 57 s. ; HUSI-STÄMPFLI et al. (n. 112), 55 ; CR LPD-MEIER/TSCHUMY, art. 5 N 49.

de manière exhaustive dans la loi (art. 5 let. c LPD)<sup>120</sup>. Parmi elles figurent les données biométriques identifiant une personne physique de manière univoque (art. 5 let. c ch. 4)<sup>121</sup>. Le critère « biométrique » est nécessaire afin d'éviter que toute photo « ordinaire » de visages ne tombe dans la notion de données sensibles, ce qui serait problématique en pratique<sup>122</sup>.

Les données biométriques désignent « les données personnelles résultant d'un traitement technique spécifique et relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique [telles que les empreintes digitales, les images faciales ou encore la voix] qui permettent ou confirment son identification unique<sup>123</sup> ». C'est notamment le cas des données qui résultent du traitement technique de la RF, si son objectif est une identification ou une authentification claire. En effet, les logiciels de RF génèrent, à partir d'images faciales<sup>124</sup>, un gabarit qui, par comparaison, permettra d'authentifier ou d'identifier une personne<sup>125</sup>.

La qualification de données comme étant des données sensibles entraîne plusieurs conséquences<sup>126</sup>. Par exemple :

- elle influence la forme du consentement qui, lorsqu'il est requis, doit être exprès pour le traitement de données sensibles (art. 6 al. 7 let. a LPD)<sup>127</sup> ;
- elle impose des obligations au responsable du traitement qui doit procéder à une analyse d'impact relative à la protection des données personnelles lors d'un traitement de données sensibles à grande échelle (art. 22 al. 1 et 2 let. a LPD) ;

- elle pose la présomption irréfragable d'une atteinte lorsque des données sensibles sont communiquées à des tiers (art. 30 al. 2 let. c LPD)<sup>128</sup> ; et
- elle impacte la pondération des intérêts (art. 31 al. 2 let. c ch. 1 et let. e ch. 2 LPD)<sup>129</sup>.

## 2. Profilage

Par profilage, il faut entendre « toute forme de traitement automatisé de données personnelles consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique » (art. 5 let. f LPD). Les critères déterminants du profilage sont donc le traitement automatisé et le but d'évaluation, c'est-à-dire un traitement impliquant un jugement de valeur, une composante subjective (p. ex. un pronostic)<sup>130</sup>. La simple collecte de données personnelles, permettant uniquement la constatation objective d'un état de fait, ne suffit pas<sup>131</sup>. Par conséquent, en fonction de l'objectif visé par la RF dans un cas d'espèce, il peut y avoir un cas de profilage.

La LPD prévoit une sous-catégorie du profilage, celle du profilage à risque élevé, qui comprend « tout profilage entraînant un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, parce qu'il conduit à un appariement de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique » (art. 5 let. g LPD). La portée de cette distinction se manifeste dans les obligations particulières déclenchées. Si l'exigence d'un consentement exprès ou d'une base légale est déjà requise pour un « simple » profilage effectué par un organe fédéral, les personnes privées traitant des données et fondant leur traitement sur le consentement ne doivent requérir le consentement exprès qu'en cas de profilage à risque élevé<sup>132</sup>.

Le profilage n'est ni plus ni moins limité par la LPD que tout autre traitement de données, et doit respecter les principes généraux du droit de la protection des données (IV.B.). Il faut notamment vérifier si les principes de finalité, de transparence et de proportionnalité sont respectés, soit en se demandant si le profilage est une mesure adap-

<sup>120</sup> CR LPD-MEIER/TSCHUMY, art. 5 N 50 ; DAVID ROSENTHAL, Das neue Datenschutzgesetz, Jusletter du 16 novembre 2020, N 23.

<sup>121</sup> La révision de la LPD a étendu la notion de données sensibles aux « données génétiques » ainsi qu'aux « données biométriques », cf. Message LPD (n. 115), FF 2017 6594. Voir également : ROSENTHAL (n. 120), N 22.

<sup>122</sup> CR LPD-MEIER/TSCHUMY, art. 5 N 52 ; ROSENTHAL (n. 120), N 22 ; SIMMLER/CANOVA, Gesichtserkennung im Strafverfahren (n. 65), 207.

<sup>123</sup> Message LPD (n. 115), FF 2017 6641.

<sup>124</sup> À noter que toutes les photographies de visages – qui sont par ailleurs des données biométriques – ne sont pas considérées comme des données sensibles au sens de la LPD. En effet, pour être qualifiées comme telles, les données doivent résulter d'un traitement technique spécifique, cf. Message LPD (n. 115), FF 2017 6541 ; HUSI-STÄMPFLI et al. (n. 112), 58.

<sup>125</sup> SIMMLER/CANOVA, Gesichtserkennung im Strafverfahren (n. 65), 207.

<sup>126</sup> Cf. CR LPD-MEIER/TSCHUMY, art. 5 N 53 pour la liste des dispositions spécifiques applicables aux données sensibles.

<sup>127</sup> Cf. IV.C.1.

<sup>128</sup> CR LPD-BOILLAT/WERLY, art. 30 N 16.

<sup>129</sup> CR LPD-MEIER/TSCHUMY, art. 5 N 53.

<sup>130</sup> ROSENTHAL (n. 120), N 24.

<sup>131</sup> ROSENTHAL (n. 120), N 24.

<sup>132</sup> MÉTILLE (n. 111), 39 ; ROSENTHAL (n. 120), N 28.

tée au but visé ou s'il est préférable de laisser l'évaluation à une personne physique<sup>133</sup>.

## B. Principes généraux

Lors de chaque traitement de données personnelles, les organes fédéraux et les personnes privées doivent respecter les principes de protection des données (art. 6 et 8 LPD), à savoir les principes de licéité, de bonne foi, de proportionnalité, de finalité, de reconnaissabilité, d'exactitude et de sécurité<sup>134</sup>. L'idée n'est pas de détailler ici le contenu de ces principes généraux, mais bien plus de les mettre en relation avec l'utilisation des technologies de RF.

Les principes de licéité, de bonne foi et de proportionnalité sont des principes généraux du droit suisse<sup>135</sup>.

Le principe de licéité, énoncé à l'art. 6 al. 1 LPD, exige que tout traitement de données soit licite dans son principe, ses modalités et son étendue<sup>136</sup>. Sa portée diffère selon que la personne responsable du traitement est une personne privée ou un organe fédéral<sup>137</sup>. La première doit s'abstenir de violer la personnalité des personnes dont les données sont traitées<sup>138</sup>, alors que le second doit respecter le principe de légalité (art. 5 al. 1 Cst. et art. 34 al. 1 LPD)<sup>139</sup>. Ces aspects seront développés dans le prochain chapitre (IV.C.).

Le principe de bonne foi (art. 6 al. 2 LPD), quant à lui, commande d'agir de manière loyale et digne de confiance dans le commerce juridique<sup>140</sup>. Les données personnelles ne doivent ainsi pas être collectées d'une manière à laquelle la personne concernée ne pouvait s'y attendre<sup>141</sup>. Cela implique en particulier d'informer de manière adéquate les personnes dont les images faciales sont utilisées ou encore d'indiquer le recours à un système de traitement automatisé (p. ex. à l'aide d'une icône de signalement)<sup>142</sup>.

En outre, le traitement des données doit être proportionné (art. 6 al. 2 LPD), c'est-à-dire qu'il doit être apte à atteindre le but poursuivi, qu'il n'existe pas de moyen moins contraignant pour atteindre ce but et qu'il est raisonnablement exigible au vu de l'atteinte à la vie privée des personnes concernées<sup>143</sup>. Dans le contexte de la RF, ce principe est important car, selon les circonstances, il devrait être possible de trouver une mesure moins incisive atteignant le but visé<sup>144</sup>. Dans le cas contraire, il convient de choisir les technologies biométriques les moins intrusives parmi celles aptes à atteindre les finalités recherchées<sup>145</sup>. Par ailleurs, les principes d'évitement et de minimisation des données<sup>146</sup> – déduits du principe de proportionnalité – sont mis à mal avec l'utilisation de technologie de RF. En effet, tant pour leur développement que pour leur fonctionnement, les logiciels ont besoin d'une grande quantité de données (« données d'apprentissage »)<sup>147</sup>.

La LPD prévoit également des principes spécifiques à la protection des données, à savoir les principes de reconnaissabilité, de finalité, d'exactitude et de sécurité<sup>148</sup>.

Le principe de reconnaissabilité (ou principe de transparence) prévoit que la collecte de données personnelles et les finalités du traitement soient reconnaissables pour la personne concernée (art. 6 al. 3 LPD). Il est concrétisé par l'art. 19 LPD qui impose un devoir d'information systématique pour la personne responsable du traitement, qu'il soit une personne privée ou un organe fédéral<sup>149</sup>. En général, pour les services proposés par des personnes privées, le principe de reconnaissabilité est respecté quand la RF constitue la prestation attendue par les usagers (p. ex. pour l'authentification avant un paiement). Le principe de reconnaissabilité peut toutefois être mis à mal lorsque l'utilisation de technologies de RF n'est pas visible, car elle passe, par exemple, par des caméras installées dans des lieux publics ou privés, et donc à l'insu des personnes concernées (si aucune icône ne mentionne un tel couplage)<sup>150</sup>. Bien que le principe de reconnaissabilité

<sup>133</sup> ROSENTHAL (n. 120), N 28.

<sup>134</sup> KARABOGA et al. (n. 19), 129.

<sup>135</sup> CR LPD-MEIER/TSCHUMY, art. 6 N 14.

<sup>136</sup> HUSI-STÄMPFLI et al. (n. 112), 84.

<sup>137</sup> HUSI-STÄMPFLI et al. (n. 112), 84.

<sup>138</sup> Elle doit s'abstenir de violer des règles relevant du droit des obligations et du droit pénal (p. ex. art. 28 CC, art. 28 CO et 146 CP, art. 29 CO et 180 s. CP), cf. CR LPD-MEIER/TSCHUMY, art. 6 N 23.

<sup>139</sup> HUSI-STÄMPFLI et al. (n. 112), 84 ; CR LPD-MEIER/TSCHUMY, art. 6 N 22. Voir également : IV.C.

<sup>140</sup> CR LPD-MEIER/TSCHUMY, art. 6 N 24.

<sup>141</sup> HUSI-STÄMPFLI et al. (n. 112), 86.

<sup>142</sup> FRA (n. 26), 27 ; YVES POULLET, L'IA un défi pour nos législations et notre vie privée, in : Astrid Epiney/Sophia Rovelli (éd.), *Künstliche Intelligenz und Datenschutz/L'intelligence artificielle et protection des données*, Zurich/Bâle/Genève 2021, 1 ss, 29.

<sup>143</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 17.

<sup>144</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 17. Voir également : III.B.3.

<sup>145</sup> PFPDT (n. 2), 14.

<sup>146</sup> Le principe d'évitement implique que si le but du traitement peut être atteint sans collecte de données nouvelles, cette option doit être privilégiée, alors que le principe de minimisation veut que seules les données absolument nécessaires au but poursuivi soient traitées, cf. MÉTILLE (n. 111), 9.

<sup>147</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 17 ; JACQUET/GROSSRIEDER (n. 7), 143.

<sup>148</sup> CR LPD-MEIER/TSCHUMY, art. 6 N 14.

<sup>149</sup> MÉTILLE (n. 111), 11.

<sup>150</sup> FRA (n. 26), 27. Au sujet de l'utilisation de la RF en temps réel dans les supermarchés suisses, voir : AlgorithmWatch, <https://>

ne soit pas absolu – et qu'il soit possible de renoncer à informer la personne concernée du traitement de données si une base légale le prévoit (p. ex. dans le domaine de la police et de la procédure pénale) – une information *a posteriori* est toujours exigée<sup>151</sup>.

Le principe de finalité, quant à lui, est étroitement lié au principe de reconnaissabilité vu que les finalités du traitement doivent être reconnaissables pour la personne concernée au moment de la collecte (art. 6 al. 3 LPD)<sup>152</sup>. Il en découle, d'une part, que les données personnelles doivent être traitées pour des finalités clairement définies (déterminabilité) et, d'autre part, que les traitements subséquents soient compatibles avec les finalités initiales (immutabilité)<sup>153</sup>. Dans le contexte de la RF, la compatibilité des finalités est mise en danger lorsqu'il y a une interopérabilité de différents systèmes reposant sur la biométrie, c'est-à-dire une interconnexion entre des bases de données personnelles<sup>154</sup>.

En ce qui concerne le principe de l'exactitude (art. 6 al. 5 LPD), celui-ci requiert de la personne responsable du traitement de données personnelles de s'assurer que ces données soient correctes, actuelles et objectives<sup>155</sup>. Cette obligation n'est pas absolue, mais doit bien plus être proportionnée à la finalité du traitement (exactitude relative des données)<sup>156</sup>. Par conséquent, les logiciels de RF doivent être entraînés par des images faciales suffisamment diversifiées en termes d'âge, de sexe et d'ethnie afin de renforcer la probabilité d'identification ou de vérification correcte<sup>157</sup>. En pratique, il peut être difficile de vérifier la façon dont un système de RF a été développé, notamment du fait qu'un algorithme basé sur un processus de *machine learning* est beaucoup moins transparent<sup>158</sup>.

Finalement, l'art. 8 LPD consacre le principe de sécurité, selon lequel les responsables du traitement et les sous-traitants doivent assurer, par des mesures organisationnelles et techniques appropriées, une sécurité adéquate des données personnelles par rapport au risque encouru (al. 1). Il s'agit dès lors de prévenir l'accès, l'utilisation et la communication non autorisés des données

traitées par les systèmes de RF, mais également d'assurer une maintenance des systèmes de RF, dont la sécurité est tributaire des sous-systèmes de stockage<sup>159</sup>.

## C. Licéité du traitement

Comment mentionné ci-dessus, tout traitement doit être licite (art. 6 al. 1 LPD). Les exigences de cette licéité varient selon que le traitement de données personnelles, respectivement le recours à la RF, est réalisé par une personne privée (art. 30 ss LPD) ou un organe fédéral (art. 33 ss LPD).

### 1. Par des personnes privées

En vertu de l'art. 30 al. 1 LPD, celui qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Sans être exhaustive, la loi prévoit trois cas de figure pour lesquels l'illicéité est donnée (art. 30 al. 2 LPD) : lorsqu'il y a violation des principes de protection des données (let. a), lorsque la personne concernée s'est opposée expressément au traitement (let. b) et lorsque des données sensibles ont été communiquées à des tiers (let. c). L'illicéité d'une atteinte peut toutefois être levée en présence d'un motif justificatif, à savoir si le consentement de la personne concernée a été donné, si un intérêt privé ou public est prépondérant ou encore si la loi le prévoit (art. 31 al. 1 LPD).

Pour qu'un consentement soit valable, ce dernier doit être libre, éclairé et déterminé (art. 6 al. 6 LPD)<sup>160</sup>. Par ailleurs, selon l'art. 6 al. 7 LPD, un consentement exprès<sup>161</sup> est nécessaire pour le traitement de données personnelles

algorithmwatch.ch/de/kennt-der-supermarkt-ihr-gesicht/, consulté le 25 mars 2025.

<sup>151</sup> ASTRID EPINEY, Allgemeine Grundsätze, in : Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (éd.), Datenschutzrecht – Grundlagen und öffentliches Recht, Berne 2011, 510 ss, N 43.

<sup>152</sup> EPINEY (n. 151), N 29 ; HUSI-STÄMPFLI et al. (n. 112), 91.

<sup>153</sup> PFPDT (n. 2), 9 ; HUSI-STÄMPFLI et al. (n. 112), 90 s.

<sup>154</sup> PFPDT (n. 2), 15.

<sup>155</sup> MÉTILLE (n. 111), 11 ; HUSI-STÄMPFLI et al. (n. 112), 96.

<sup>156</sup> MÉTILLE (n. 111), 11 ; HUSI-STÄMPFLI et al. (n. 112), 96.

<sup>157</sup> BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 20. Voir également : III.A.

<sup>158</sup> JACQUET/GROSSRIEDER (n. 7), 143.

<sup>159</sup> FRA (n. 26), 29 ; PFPDT (n. 2), 19.

<sup>160</sup> Un consentement est libre dans la mesure où il ne doit pas être obtenu sous la pression ou la menace, et il est éclairé s'il fait suite à une information appropriée, objective et compréhensible, cf. CR LPD-BOILLAT/WERLY, art. 31 N 21. Pour plus de détails concernant la notion du consentement dans la LPD, voir : TOBIAS FASNACHT, Die Einwilligung im Datenschutzrecht, thèse Fribourg, Zurich/Bâle/Genève 2017, 96 ss.

<sup>161</sup> Selon le Message du Conseil fédéral, « une déclaration de volonté est « expresse » lorsqu'elle est formulée oralement, par écrit ou par un signe, et qu'elle découle directement des mots employés ou du signe en question. [...] Cela pourrait se faire notamment en cochant une case, en optant activement pour certains paramètres techniques pour des services de la société de l'information ou au moyen d'une autre déclaration. La même chose vaudrait pour des moyens d'expression non verbaux qui, dans le contexte concret, sont des signes clairs, ou un geste approprié, ce qui peut être fréquemment le cas lors d'une consultation médicale. On peut par exemple penser à des signes approuvateurs de la tête ou à l'ouverture de la bouche pour le prélèvement de muqueuse, après des explications claires. », cf. Message LPD (n. 115), FF 2017 6648.

sensibles (let. a) ainsi que pour le profilage à haut risque par une personne privée (let. b). Par conséquent, l'atteinte à la personnalité induite par l'utilisation de la RF ne peut être justifiée par le consentement de la personne concernée que si cette dernière y a consenti expressément. En effet, comme la RF génère des données personnelles sensibles – et, selon les circonstances, peut même constituer un profilage à risque élevé<sup>162</sup> –, seul un consentement exprimé d'une manière apparente, comme une signature ou une déclaration verbale non équivoque peut être pris en compte<sup>163</sup>.

Dans le secteur privé, la licéité du traitement repose principalement sur le consentement, ce dernier étant souvent nécessaire afin de pouvoir bénéficier du service en question. Se pose alors la question de savoir si les exigences d'un consentement libre et éclairé peuvent être remplies, dans la mesure où un refus conduit à un nonaccès au service, et que la complexité du fonctionnement des systèmes de RF rend difficile la compréhension de la portée du consentement<sup>164</sup>. L'absence d'alternative pour une prestation et la complexité des informations – souvent contenues dans des conditions générales rarement lues<sup>165</sup> – démontrent les limites du consentement, qui consiste bien souvent en une fiction juridique.

L'intérêt prépondérant de la personne responsable du traitement peut également fonder un motif justificatif. Cet intérêt au traitement de données doit être mis en balance avec l'intérêt de la personne concernée à ne pas voir ses données personnelles traitées. Il n'est pas admis facilement mais peut, dans certain cas, justifier une atteinte. La LPD fournit à l'art. 31 al. 2 une liste non exhaustive<sup>166</sup> des cas dans lesquels l'intérêt de la personne responsable de traitement est susceptible d'être prépondérant<sup>167</sup>. Ces exemples ont valeur de présomption ; c'est le résultat de la pesée des intérêts dans le cas d'espèce qui est déterminant<sup>168</sup>.

Comme les données biométriques générées par la RF sont à qualifier de données personnelles sensibles<sup>169</sup>, cette qualité influence la pondération des intérêts. En effet, l'intérêt poursuivi par la personne privée doit être particulièrement important, ce qui exclut *a priori* un intérêt purement économique. Par exemple, l'intérêt de la personne responsable du traitement n'est pas prépondérant lorsque le but du traitement est d'évaluer la solvabilité de la personne concernée (cf. art. 31 al. 2 let. c ch. 1 LPD).

## 2. Par des organes fédéraux

En principe, les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale (art. 34 al. 1 LPD). Ce n'est que dans des cas exceptionnels qu'une base légale peut faire défaut (cf. art. 35, 36 et 39 LPD)<sup>170</sup>. L'art. 34 al. 1 LPD concrétise non seulement le principe de légalité prévu dans la Constitution fédérale (art. 5 al. 1 Cst.), mais assure également une protection de la personnalité et des droits fondamentaux (cf. art. 1 LPD)<sup>171</sup>. En effet, l'art. 36 al. 1 1<sup>re</sup> phrase Cst. prévoit que toute restriction d'un droit fondamental doit reposer sur une base légale (III.B.1.).

En vertu de l'art. 34 al. 2 LPD, une base légale au sens formel est requise lorsqu'il s'agit d'un traitement de données sensibles (let. a), d'un profilage (let. b) ou lorsque la finalité ou le mode du traitement de données personnelles est susceptible de porter gravement atteinte aux droits fondamentaux de la personne concernée (let. c). L'utilisation de la RF nécessite ainsi une base légale au sens formel. En effet, les logiciels de RF produisent des données personnelles sensibles, peuvent être utilisés à des fins de profilage et sont susceptibles de porter gravement atteinte aux droits fondamentaux (III.B.1. et IV.A.1.).

*À titre d'exemple, l'Office fédéral de la police (fedpol) étendra à partir de 2026 le système automatique d'identification des empreintes digitales (AFIS) à la reconnaissance faciale<sup>172</sup>. Pour ce faire, fedpol se base sur l'art. 345 CP<sup>173</sup> qui prévoit la collaboration entre autorités à des fins d'identification de personnes et qui constitue la base*

<sup>162</sup> Voir : IV.A.

<sup>163</sup> Il n'est toutefois pas nécessaire que le consentement soit donné sous la forme écrite, cf. CR LPD-MEIER/TSCHUMY, art. 6 N 96.

<sup>164</sup> POULLET (n. 142), 31

<sup>165</sup> Toutefois, des clauses insolites (inattendues) ou abusives (disproportionnées) sont considérées comme illégales, même si la personne y a consenti, cf. SYLVAIN MÉTILLE, <https://smetille.ch/2014/11/20/protection-des-donnees-tout-savoir-sur-le-consentement/>, consulté le 25 mars 2025.

<sup>166</sup> Message LPD (n. 115), FF 2017 6689.

<sup>167</sup> C'est le cas, par exemple, des données personnelles qui sont traitées à des fins ne se rapportant pas à des personnes – notamment dans le cadre de la recherche, de la planification ou de la statistique – et qui sont anonymisées (art. 31 al. 2 let. e pt. 1 à 3 LPD).

<sup>168</sup> CR LPD-BOILLAT/WERLY, art. 31 N 30 ; BRAUN BINDER/KUNZ/OBRECHT (n. 13), N 23.

<sup>169</sup> Voir : IV.A.

<sup>170</sup> CR LPD-EPINEY/POSSE, art. 34 N 3.

<sup>171</sup> CR LPD-EPINEY/POSSE, art. 34 N 3.

<sup>172</sup> Conseil fédéral, <https://www.fedpol.admin.ch/fedpol/fr/home/aktuell/mm.msg-id-94141.html>, consulté le 25 mars 2025 ; Office fédéral de la police, FAQ – AFIS2026, 2 (disponible sous : <https://www.fedpol.admin.ch/dam/fedpol/fr/data/sicherheit/personenidentifikation/afis/faq-afis2026.pdf.download.pdf/faq-afis2026-f.pdf>).

<sup>173</sup> Code pénal suisse du 21 décembre 1937 (CP ; RS 311.0).

*légale du AFIS, sur l'art. 14 al. 2 LSIP<sup>174</sup> qui permet à fedpol de traiter des images faciales, ainsi que sur l'art. 2 let. c de l'ordonnance sur le traitement des données signalétiques biométriques<sup>175</sup>. À noter que le système comparera uniquement les images enregistrées dans le système AFIS (RF a posteriori), toute surveillance automatisée de personnes en temps réel, par exemple par des caméras installées dans l'espace public, étant exclue<sup>176</sup>.*

## V. Conclusion

Le cadre légal instauré par les droits fondamentaux ainsi que par le droit de la protection des données assure aux individus une certaine protection contre des ingérences de l'État dans leur sphère privée et des atteintes liées à un traitement de données personnelles les concernant. Les logiciels d'IA et de RF évoluant rapidement, il est important que le cadre légal soit « technologiquement neutre » pour assurer une sécurité du droit.

Certains principes sont toutefois difficiles à respecter lorsqu'il est fait usage de la RF dans un but d'identification (« 1-v-N »), notamment en raison de son mode de fonctionnement (traitement de masse automatisé et systématique). Un encadrement plus spécifique serait souhaitable dans certaines constellations, notamment en raison des risques que cette technologie comporte pour les droits fondamentaux. Par exemple, le renforcement de l'obligation d'informer, ou de rendre visible, lorsqu'il est fait usage de cette technologie dans des lieux publics, mais également dans ceux qui sont accessibles au public (comme les centres commerciaux, les stades ou les hôpitaux) nous paraît opportun.

Une approche plus restrictive a été adoptée par certains cantons et villes, dont Zurich, Saint-Gall, Lausanne et Bâle-Ville, qui ont accepté des interventions visant à interdire la reconnaissance faciale dans les espaces publics<sup>177</sup>. Par ailleurs, le règlement européen sur l'IA<sup>178</sup> interdit les

systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance (art. 5 par. 1 let. e). Même si ce règlement n'est pas directement applicable en Suisse, il déploie tout de même un effet extraterritorial et s'applique aux entreprises suisses qui exportent des systèmes d'intelligence artificielle sur le marché de l'UE ou qui développent et fournissent des systèmes d'intelligence artificielle utilisés dans l'UE (cf. art. 2 règlement européen sur l'IA).

<sup>174</sup> Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP ; RS 361).

<sup>175</sup> Ordonnance du 6 décembre 2013 sur le traitement des données signalétiques biométriques (RS 361.3).

<sup>176</sup> Office fédéral de la police, <https://www.ejpd.admin.ch/fedpol/fr/home/sicherheit/personenidentifikation-neu/gesichtsbild-abgleich.html>, consulté le 25 mars 2025.

<sup>177</sup> AlgorithmWatch, <https://algorithmwatch.ch/fr/grands-succes/>, consulté le 4 janvier 2025 ; Amnesty, <https://www.amnesty.ch/fr/pays/europe-asie-centrale/suisse/docs/2023/plusieurs-villes-et-cantons-veulent-interdire-la-reconnaissance-faciale>, consulté le 4 janvier 2025.

<sup>178</sup> Règlement (UE) 2024/1689 du 13 juin 2024 sur l'intelligence artificielle (JO L 2024/1689 du 12 juillet 2024).