Droit de la reconnaissance faciale ou biométrique

Actualité législative publié le **05/10/2022**, vu **500 fois**, Auteur : Jérôme CHAMBRON, BAC+4 en Droit

Droit de la reconnaissance faciale ou biométrique

Les citations de textes en italique proviennent :

- soit du site internet de la Commission nationale informatique et libertés ou CNIL, signalé en fin de citation par ceci : **(1)**
- soit de la Direction de l'Information Légale et Administrative ou DILA, Légifrance (CSI ou code de la sécurité intérieure, code pénal, Code civil), signalé en fin de citation par ceci : **(2)**

Les textes juridiques cités dans l'exposé sont ceux en vigueur à la date du 01/07/2022.

Les abréviations utilisées dans l'exposé sont expliquées ci-après :

RGPD : règlement général de la protection des données. Il s'agit d'un règlement européen.

En droit européen on a principalement quatre types de textes :

1. les règlements : ils sont normatifs. Il s'agit de textes impersonnels, généraux et impératifs dès leur publication au journal officiel ou JO. Ils sont équivalents aux lois en France.
2. les directives : les directives fixent des objectifs à atteindre et les États sont libres des moyens à employer pour arriver au but. Si elles ne sont pas transposées dans les délais elles deviennent impératives dans leur principe et invoquables par les justiciables.
3. les recommandations : textes sans force contraignante.
4. les avis : textes sans force contraignante.

TAJ : traitement des antécédents judiciaires. Fichier commun entre Police et Gendarmerie.

Figurent dans le TAJ les personnes ayant été condamnées pénalement ainsi que les personnes non condamnées pénalement mais ayant été soupçonnées d'avoir commis une ou plusieurs infractions.

CSI : code de la sécurité intérieure.

Le plan de l'exposé :

Introduction

Section 1 - Les contours de la reconnaissance faciale ou biométrique

§ 1 - Le principe est celui de l'interdiction de la reconnaissance faciale ou biométrique

- Le RGPD article 9, §1

§ 2- Les exceptions au principe d'interdiction de la reconnaissance faciale ou biométrique

- Le RGPD article 9, §2

§ 3 - Les analyses d'impact imposées par la CNIL

Section 2 - Les limites de la reconnaissance faciale ou biométrique

§ 1 - La vidéoprotection publique et la vidéosurveillance privée

1 - Les limites à la vidéoprotection publique

2 - Les limites à la vidéosurveillance privée

a - Les limites par le droit civil

- L'article 9 du Code civil

b - Les limites par le droit pénal

- L'article 226-1 du code pénal

- L'article 226-2 du code pénal

§ 2 - Les sanctions pouvant être prononcées par la CNIL

Conclusion

Introduction :

Je commencerai mon propos par la citation de l'article premier de la loi informatique et liberté n° 78-17 du 6 janvier 1978. Je cite :

> *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.***(2)**

Ensuite, la *reconnaissance faciale* ne doit pas être confondue avec la *détection de visage* qui caractérise la présence ou non d'un visage dans une image indépendamment de la personne à qui il appartient.

En ce qui concerne la reconnaissance faciale ou biométrique, elle représente un marché à haut potentiel. Selon une étude récente, le poids du marché de la reconnaissance faciale en 2022 sera de 9,5 milliards de dollars.

La reconnaissance faciale est une donnée biométrique dont voici une définition :

RGPD, article 4, §14 :

> Sont des *«données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des* ***images faciales*** *ou des données dactyloscopiques;* **(1)**

Section 1 - Les contours de la reconnaissance faciale ou biométrique

§ 1 - Le principe est celui de l'interdiction de la reconnaissance faciale ou biométrique

- Le RGPD article 9, §1

> ***Le traitement des données à caractère personnel*** *qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques,* ***des données biométriques aux fins d'identifier une personne physique de manière unique****, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* ***sont interdits****.* **(1)**

§ 2- Les exceptions au principe d'interdiction de la reconnaissance faciale ou biométrique

- Le RGPD article 9, §2

> *a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;*
>
> *b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;*
>
> *c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;*
>
> *d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;*

e) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. **(1)**

Parmi les autres exceptions, on a la police administrative et la police judiciaire.

La police administrative agit en prévention des infractions pénales tandis que la police judiciaire, ou PJ, a pour but la recherche et la poursuite des auteurs d'infractions pénales. Le TAJ fait ainsi exception au principe d'interdiction de la reconnaissance faciale. Il comprend environ un peu moins de 20 millions de fiches individuelles.

Enfin, il est permis la reconnaissance faciale sur les smatphones, les ordinateurs, et dans les centrales nucléaires par exemple.

§ 3 - Les analyses d'impact imposées par la CNIL

La CNIL impose des analyses d'impact concernant la protection des données (AIPD) des personnes dites « *vulnérables* » : élèves, personnes âgées, patients, employés, demandeurs d'asile, etc...

Dès lors que la mise en œuvre d'un dispositif de vidéoprotection conduit à « *la surveillance systématique à grande échelle d'une zone accessible au public*», type de traitements expressément mentionné à l'article 35.1 du RGPD comme susceptible de présenter « *un risque élevé pour les droits et libertés des personnes physiques* », une AIPD doit être effectuée.

Par ce biais, une évaluation de la nécessité et de la proportionnalité du dispositif envisagé, au regard des finalités poursuivies, est opérée avant son implantation.

Dans les grandes entreprises et dans les communes, quelle que soit leur taille, on trouve un délégué à la protection des données (DPO).

> *Quel est le montant des sanctions prévues par le règlement en cas de manquements aux dispositions relatives aux analyses d'impact ?*
>
> *Le montant des amendes peut s'élever jusqu'à 10 000 000 euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83(4)(a)).* **(1)**

L'AIPD se déclare en ligne sur le site internet de la CNIL par la personne morale concernée.

Section 2 - Les limites de la reconnaissance faciale ou biométrique

§ 1 - La vidéoprotection publique et la vidéosurveillance privée

1 - Les limites à la vidéoprotection publique

Elle est soumise à autorisation préfectorale et la conservation des données est d'1 mois maximum (L252-5 du CSI) sauf pour les besoins d'un procès pénal auquel cas on conserve les données pour servir de preuve.

Code de la sécurité intérieure ou CSI, article L. 242-4 alinéa 2, citation d'un extrait relatif aux aéronefs sans personne à bord, communément appelés drônes :

> *Les dispositifs aéroportés ne peuvent ni procéder à la captation du son,* ***ni comporter de traitements automatisés de reconnaissance faciale*** *. Ces dispositifs ne peuvent procéder à aucun rapprochement, interconnexion ou mise en relation automatisé avec d'autres traitements de données à caractère personnel.* **(2)**

2 - Les limites à la vidéosurveillance privée

a - Les limites par le droit civil

- L'article 9 du Code civil

Chacun a droit au respect de sa vie privée.

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. **(2)**

b - Les limites par le droit pénal

- L'article 226-1 du code pénal

Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, ***des paroles prononcées à titre privé ou confidentiel*** *;*

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, ***l'image d'une personne se trouvant dans un lieu privé****.*

3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.

Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale.

Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende. **(2)**

- L'article 226-2 du code pénal

Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.

Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. **(2)**

§ 2 - Les sanctions pouvant être prononcées par la CNIL

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut prononcer, après une procédure contradictoire , l'une ou plusieurs des mesures suivantes :

- *Un rappel à l'ordre.*
- *Une injonction de se mettre en conformité. Cette injonction peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 euros par jour de retard.*
- *Une limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation.*
- *Le retrait d'une certification.*
- *La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale.*
- *Une suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes (BCR).*
-

Une amende administrative ne pouvant excéder 10 millions d'euros ou 2% du chiffre d'affaire annuel mondial de la société. Pour les manquements les plus graves, ce montant peut s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.

À noter : *La formation restreinte peut décider de rendre publique la décision qu'elle adopte. Elle peut également ordonner l'insertion, aux frais des organismes sanctionnés, de la décision dans des publications, journaux et supports qu'elle désigne. (site internet de la CNIL)* **(1)**

Ainsi, à la fin de l'année 2021, la société privée Clearview AI, a été mise en demeure sous 2 mois, de ne plus « aspirer » des photos sur internet à des fins de reconnaissance faciale. En effet, elle s'est approprié plus de 10 milliards d'images à travers le monde qu'elle revend, entre autres, aux forces de l'ordre.

En conséquence, la présidente de la CNIL ***a décidé de mettre la société CLEARVIEW AI en demeure*** *de :*

- *cesser la collecte et l'usage des données de personnes se trouvant sur le territoire français en l'absence de base légale ;*
- *faciliter l'exercice des droits des personnes concernées et de faire droit aux demandes d'effacement formulées.*

La société CLEARVIEW AI dispose d'un délai de deux mois pour respecter les injonctions formulées dans la mise en demeure et en justifier auprès de la CNIL. Si, à l'issue de ce délai, elle ne s'est pas conformée, la présidente de la CNIL aura la possibilité de saisir la formation restreinte de la CNIL qui pourra prononcer une sanction, notamment pécuniaire. **(1)**

Conclusion :

Concernant la France, il est préconisé une large concertation et un grand débat public sur la question de la reconnaissance faciale qui devrait ensuite déboucher sur une nouvelle loi.

Au niveau communautaire, le Comité européen de la protection des données ou CEPD, préconise pour l'avenir une interdiction :

- *de l'identification biométrique à distance des individus dans les espaces accessibles au public ;*
- *des systèmes de reconnaissance faciale qui classent les individus sur la base de leurs données biométriques dans des groupes en fonction de l'ethnie, du sexe, de l'orientation politique ou sexuelle ou d'autres motifs de discrimination ;*
- *de la reconnaissance faciale ou des technologies similaires permettant de déduire les émotions d'une personne physique ;*
- *du traitement de données personnelles dans un contexte répressif qui s'appuierait sur une base de données alimentée par la collecte de données personnelles à grande échelle et de manière indiscriminée, par exemple en collectant des photographies et des images faciales accessibles en ligne.*

Ces lignes directrices seront soumises à une consultation publique d'une durée de 6 semaines. **(1)**

POUR ALLER PLUS LOIN :

https://www.legavox.fr/blog/jerome-chambron/reconnaissance-faciale-biometrique-regles-vigueur-32521.htm