Décision MED-2021-134 du 26 novembre 2021

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Mise en demeure
Etat juridique : En vigueur

Date de publication sur Légifrance : Jeudi 16 décembre 2021

Décision n° MED-2021-134 du 26 novembre 2021 mettant en demeure la société X

(N° MDM211166)

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 20 ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-116C du 26 août 2020 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société X ;

Vu les saisines n° X ;

Vu le questionnaire de contrôle sur pièces du 27 octobre 2020 ;

Vu les autres pièces du dossier ;

La procédure

La société X (ci-après ' la société ' ou ' X '), établie aux États-Unis, a été créée en 2017. Elle a développé un logiciel de reconnaissance faciale, dont la base de données repose sur l'aspiration de photographies publiquement accessibles sur Internet, qui permet d'identifier une personne à partir d'une photographie la représentant.

La Commission nationale de l'informatique et des libertés (ci-après ' CNIL ') a été saisie entre mai et décembre 2020 de plusieurs réclamations relatives aux difficultés rencontrées par les plaignants pour exercer leurs droits d'accès et d'effacement auprès de la société.

En application de la décision n° 2020-116C du 26 août 2020 de la Présidente de la CNIL, une délégation de la CNIL a procédé à une mission de contrôle sur pièces par l'envoi d'un questionnaire le 27 octobre 2020, auquel la société a répondu par un courrier du 27 novembre suivant. Ce questionnaire portait sur les différents traitements mis en œuvre par la société, les organismes utilisateurs des services de la société (actuels ou anciens) ayant leur principal établissement en France ou au sein de l'Union européenne ainsi que les réclamations n° X.

Le 27 mai 2021, la CNIL a été saisie d'une plainte de l'organisme Privacy International (saisine n° X) portant sur le logiciel de reconnaissance faciale de la société et son utilisation par les forces de l'ordre.

Dans le cadre de l'assistance mutuelle prévue à l'article 61 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le ' RGPD ' ou le ' Règlement), la CNIL s'est vue communiquer des informations utiles par plusieurs de ses homologues européens.

Le contexte

Il ressort des informations utiles, transmises dans le cadre de la coopération entre autorités de contrôle, d'informations publiquement accessibles ainsi que des réclamations reçues par la Commission que la société utilise une technologie propre pour indexer les pages web librement accessibles. Elle collecte toutes les images sur lesquelles apparaissent des visages, sur des millions de sites web. Des photographies sont ainsi extraites notamment de réseaux sociaux (par exemple, Twitter ou Facebook), de sites professionnels contenant des photographies de leurs salariés, de blogs et de tous sites sur lesquels des photographies de personnes sont publiquement accessibles. Des images sont également extraites de vidéos disponibles en ligne, par exemple sur le site www.youtube.com. Cette collecte concerne des images de personnes majeures comme mineures, aucun filtre n'étant appliqué à cet égard. Seules des centaines d'URL, associées aux sites ' pour adultes ' ayant des audiences parmi les plus importantes, sont bloquées et exclues de la collecte.

La collecte de ces images sur des réseaux sociaux porte sur l'ensemble des images accessibles au moment de la collecte à une personne non connectée au réseau en cause. En dehors des réseaux sociaux, la collecte concerne l'ensemble des images accessibles au moment de la collecte à un moteur de recherche. La société a ainsi collecté plus de dix milliards d'images.

À partir de chaque photographie collectée, la société calcule un gabarit biométrique. Une empreinte numérique unique, propre au visage tel qu'il apparaît sur la photographie (basée sur les points du visage) est ainsi générée. Les milliards d'images sont ensuite enregistrées dans une base de données sous une forme permettant de les rechercher (à l'aide de l'empreinte numérique).

La société commercialise l'accès à une plateforme en ligne sur laquelle se trouve un moteur de recherche. Cet outil fonctionne en y téléchargeant une photographie d'un visage. À partir de cette photographie, l'outil calcule l'empreinte numérique correspondante à celle-ci et effectue, dans la base de données, une recherche des photographies auxquelles sont liées des empreintes similaires. Le logiciel produit un résultat de recherche, composé de photographies, auxquelles est associé l'URL de la page web à partir de laquelle elles ont été extraites (réseau social, article de presse, blog …). Ce résultat de recherche compile ainsi l'ensemble des images collectées par la société au sujet d'une personne ainsi que le contexte dans lequel ces images sont en ligne, tel que, par exemple, le compte de réseau social ou un article de presse.

La société décrit le service qu'elle offre comme ' un outil de recherche utilisé par les forces de l'ordre (' law inforcement ') pour identifier des auteurs et des victimes d'infractions ' à partir d'une photographie. Il est indiqué sur son site web que cet outil permet par exemple à des ' analystes ' d'effectuer une recherche en téléchargeant des images de scènes de crime afin de les comparer à celles qui sont publiquement accessibles. Les forces de l'ordre peuvent ainsi utiliser cet outil afin d'identifier une personne dont elles disposent d'une image (par exemple, issue d'un enregistrement de vidéosurveillance) mais ne connaissent pas l'identité.

Sur l'applicabilité du RGPD

En vertu de l'article 3, paragraphe 2 du RGPD : ' Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : […] b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. ' (soulignement ajouté).

Le considérant 24 du RGPD précise à cet égard que ' Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit ' (soulignement ajouté).

À titre d'éclairage, dans ses lignes directrices 3/2018 relatives au champ d'application territorial du RGPD dans leur version du 12 novembre 2019, le Comité européen de protection des données (ci-après ' le CEPD ') relève que, ' contrairement à la disposition de l'article 3, paragraphe 2, point a), ni l'article 3, paragraphe 2, point b), ni le considérant 24 n'introduisent expressément un degré nécessaire d' ' intention de cibler ' de la part du responsable du traitement ou du sous-traitant pour déterminer si l'activité de surveillance déclencherait l'application du RGPD aux activités de traitement. Toutefois,

l’utilisation du mot ' suivi ' implique que le responsable du traitement poursuit un objectif spécifique en vue de la collecte et de la réutilisation ultérieure des données pertinentes relatives au comportement d’une personne au sein de l’Union. Le comité n’estime pas que la collecte ou l’analyse en ligne de données à caractère personnel relatives à des personnes dans l'Union serait automatiquement considérée comme un ' suivi '. Il sera nécessaire de tenir compte de la finalité du traitement des données par le responsable du traitement et, en particulier, de toute analyse comportementale ou technique de profilage ultérieure impliquant ces données. Le comité tient compte du libellé du considérant 24, qui indique que pour déterminer si le traitement implique le suivi du comportement d'une personne concernée, le suivi des personnes physiques sur l’internet, y compris l’utilisation ultérieure potentielle de techniques de profilage, constitue un facteur important '.

Dans la mesure où la société n’est pas établie dans l’Union européenne, il convient donc, pour que le RGPD soit applicable au traitement en cause, de déterminer si le traitement concerne des données à caractère personnel relatives à des personnes concernées sur le territoire de l’Union européenne et si le traitement est lié au suivi du comportement de ces personnes.

En premier lieu, il ressort de la politique de confidentialité de la société jointe en annexe que la société collecte notamment :

des photographies publiquement accessibles sur Internet ;

les informations qui peuvent être extraites de ces photographies, telles que les métadonnées de géolocalisation que la photographie peut contenir ;

les informations dérivées de l’apparence faciale des personnes figurant sur ces photographies.

Ces trois catégories de données constituent des données à caractère personnel de la personne dont le visage apparaît sur la photographie en cause. En effet, la notion de donnée à caractère personnel est définie dans le RGPD comme ' toute information se rapportant à une personne physique identifiée ou identifiable […] ', cette identification pouvant se rapporter notamment ' à un ou plusieurs éléments spécifiques propres à son identité physique '. L’image de la personne photographiée ou filmée constitue une donnée à caractère personnel dès que la personne est identifiable, c'est-à-dire qu’elle peut être reconnue. En outre, cette image peut être comparée (par un procédé automatisé ou non) avec une image détenue par ailleurs et rattachée à une personne identifiée et l’identité de cette personne peut être déduite. La société traite également des données biométriques associées à ces images.

Par ailleurs, les images collectées concernent des personnes situées dans l’Union européenne. En effet, cette collecte n’est pas limitée géographiquement au territoire américain sur lequel est établi la société, puisque ces données sont collectées sur Internet, notamment à partir de réseaux sociaux mondiaux. La CNIL relève que, dans le cadre de ses réponses au questionnaire transmis par la délégation de contrôle, la société reconnaît traiter des données à caractère personnel de résidents européens, notamment en affirmant accéder à l’ensemble des demandes d’accès et d’opposition formulées par des résidents de l’Union européenne. En particulier, des personnes situées en France ont été concernées par le traitement en cause puisque la CNIL a été saisie de trois réclamations par des personnes résidant en France portant sur les difficultés rencontrées dans l’exercice de leur droit d’accès et d’opposition auprès de la société.

Par conséquent, la société traite des données à caractère personnel de personnes physiques situées dans l’Union européenne et, en particulier, en France.

En second lieu, afin d’établir si l’activité de traitement en cause peut être considérée comme liée au suivi du comportement des personnes concernées au sens de l’article 3 du RGPD, il y a lieu de déterminer si les personnes physiques font l’objet d’un suivi sur Internet.

Conformément au considérant 24 du RGPD, la notion de suivi sur Internet comprend l’utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d’une personne physique. Le profilage est défini à l’article 4 du RGPD comme ' toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique '. Il faut par ailleurs souligner que l’article 3 du RGPD n’exige pas que le traitement ait pour finalité un suivi du comportement des personnes mais y soit simplement ' lié '.

Il y a lieu de relever à titre liminaire que les opérations de traitements mises en œuvre par la société afin de collecter des données et de constituer une base de données, à laquelle un moteur de recherche accède pour fournir un résultat sont ici analysées globalement, au regard de leur finalité commune, qui est de commercialiser un moteur de recherche fondé sur la reconnaissance faciale (ci-après ' le traitement ').

Premièrement, le traitement en cause amène à la création d’un profil comportemental de l’ensemble des personnes dont les données sont collectées.

Il ressort des informations utiles, transmises dans le cadre de la coopération entre autorités de contrôle, que l'outil en cause permet de générer, à partir d'une photographie, un résultat de recherche contenant l'ensemble des photographies ayant un gabarit biométrique suffisamment proche de celle-ci. Ce résultat de recherche comprend l'ensemble des photographies sur lesquelles le visage d'une personne apparaît et qui ont été collectées par la société, sous réserve d'une marge d'erreur technique.

Le profil ainsi créé, relatif à une personne, est composé de photographies mais également de l'adresse URL de l'ensemble des pages web sur lesquelles se trouvent ces photographies. Or, la mise en relation des photographies et du contexte dans lequel elles sont présentées sur un site web permet de recueillir de nombreuses informations sur une personne, ses habitudes ou ses préférences. S'agissant en particulier des réseaux sociaux, une photographie ainsi que l'URL d'origine de cette photographie sont fortement susceptibles de permettre d'identifier le compte de la personne concernée. Les photographies peuvent également avoir été mises en ligne afin d'illustrer un article de presse ou de blog, qui est dès lors susceptible de contenir des informations précises relatives à la personne concernée et ainsi des éléments ayant trait à son comportement.

En outre, les images peuvent contenir des métadonnées, telles que les métadonnées de géolocalisation, qui sont également comprises dans le résultat d'une recherche et permettent de compléter le profil d'une personne.

Un tel résultat de recherche permet également d'identifier le comportement d'une personne sur Internet, par l'analyse des informations que cette personne a choisi de mettre en ligne ainsi que leur contexte. En effet, la mise en ligne de photographies constitue en soi un comportement de la personne concernée, en reflétant des choix sur le niveau d'exposition qu'elle souhaite donner à des éléments de sa vie privée ou professionnelle.

Par conséquent, il convient de considérer que le résultat de recherche qui est associé à une photographie doit être qualifié, au moins en partie, de profil comportemental de la personne concernée dans la mesure où il contient de nombreuses informations relatives à cette personne et en particulier à son comportement. À supposer même que la finalité elle-même du traitement ne soit pas le suivi comportemental, les moyens mis en œuvre pour permettre le système d'identification biométrique de la société X implique la constitution d'un tel profil, et le traitement peut être regardé comme ' lié au suivi du comportement ' des personnes concernées.

Deuxièmement, le traitement automatisé de données permettant la création de ce profil comportemental et sa mise à disposition des personnes effectuant les requêtes dans le moteur de recherche de la société doit être qualifié de suivi sur Internet.

En effet, la finalité même de l'outil commercialisé par X est de pouvoir identifier et recueillir certaines informations relatives à une personne. La mise en œuvre des différentes étapes des traitements décrits supra, et notamment de techniques biométriques permettant de singulariser un individu, amènent à la création d'un profil comportemental. Or, ce profil est créé en réponse à une recherche effectuée par une personne et relative à un individu figurant sur une photographie.

En outre, la recherche peut être renouvelée dans le temps, ce qui permet de constater une évolution des informations relatives à une personne, notamment si les résultats des recherches successives sont comparés. En effet, la base de données étant mise à jour régulièrement, des recherches successives permettent de suivre l'évolution d'un profil dans le temps.

Par conséquent, le fait qu'une recherche ponctuelle permette, à tout moment, l'accès au profil d'une personne tel que décrit précédemment doit être considéré comme le suivi du comportement de personnes.

Le traitement ainsi mis en œuvre est donc lié au suivi du comportement des personnes concernées au sens des dispositions de l'article 3.2.b) du RGPD et ressortit du champ d'application territorial du RGPD.

Sur la compétence de la CNIL et l'absence d'applicabilité du mécanisme de guichet unique

L'article 55.1 du RGPD dispose que ' chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'Etat membre dont elle relève '.

L'article 56.1 prévoit : ' Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60. '

Le considérant 122 du RGPD précise : ' Chaque autorité de contrôle devrait être compétente sur le territoire de l'État membre dont elle relève pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement. Cela devrait couvrir, notamment, […] le traitement effectué par un responsable du traitement ou un sous-

traitant qui n'est pas établi dans l'Union lorsque ce traitement vise des personnes concernées résidant sur le territoire de l'État membre dont elle relève. […] '

Il ressort d'une lecture combinée des articles 55 et 56 du RGPD que, dans l'hypothèse où un responsable de traitement implanté en dehors de l'Union européenne met en œuvre un traitement transfrontalier soumis au RGPD mais qu'il n'y dispose ni d'administration centrale, ni d'établissement doté d'un pouvoir décisionnel quant à ses finalités et à ses moyens, le mécanisme du guichet unique prévu à l'article 56 du RGPD n'a pas vocation à s'appliquer. Chaque autorité de contrôle nationale est donc compétente pour contrôler le respect du RGPD sur le territoire de l'Etat membre dont elle relève.

En l'espèce, la société est établie aux États-Unis d'Amérique et ne dispose d'aucun établissement sur le territoire d'un État membre de l'Union européenne.

Par conséquent, le mécanisme du guichet unique n'est pas applicable et la CNIL est compétente pour veiller, sur le territoire français, à ce que les traitements soient mis en œuvre conformément aux dispositions du RGPD.

Sur les manquements au RGPD

Un manquement à l'obligation de disposer d'une base juridique pour les traitements mis en œuvre

L'article 6 du Règlement général sur la protection des données dispose que : ' Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant. '

Pour être licite, un traitement de données à caractère personnel doit donc reposer sur l'une des bases juridiques visées ci-dessus.

Il ressort des informations utiles transmises dans le cadre de la coopération entre autorités de contrôle que le logiciel de reconnaissance faciale mis en œuvre par la société repose sur la collecte systématique et généralisée, à partir de millions de sites web à travers le monde, d'images contenant des visages, à l'aide d'une technologie exclusive pour indexer les pages web librement accessibles.

La société procède ensuite à un traitement des données collectées afin de constituer une base de données et de permettre la recherche des photographies dans cette base à partir d'une autre image.

Ce traitement est réalisé par la société à des fins exclusivement commerciales.

Dans le cadre des investigations menées par la CNIL, la société a été interrogée sur le fondement juridique de ce traitement, au sens de l'article 6 du RGPD. La société n'a apporté aucune réponse sur ce point. La politique de confidentialité de la société, précédemment évoquée, n'évoque pas davantage le fondement juridique dudit traitement.

Il peut être relevé d'emblée que la société n'a pas recueilli le consentement des personnes concernées au traitement de leurs données à caractère personnel.

En outre, compte tenu de la nature des traitements en cause, les fondements juridiques prévus par les dispositions de l'article 6.1 sous b), c), d) et e), du RGPD et liés à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique et à l'exécution d'une mission d'intérêt public ne trouvent pas à s'appliquer en l'espèce.

En ce qui concerne le fondement juridique lié aux intérêts légitimes poursuivis par le responsable de traitement, prévu par l'article 6. 1. f) du Règlement, il y a lieu de rappeler à titre liminaire que le caractère ' publiquement accessible ' d'une donnée n'influe pas sur la qualification de donnée à caractère personnel et qu'il n'existe aucune autorisation générale permettant de réutiliser et de traiter de nouveau des données à caractère personnel publiquement disponibles, en particulier à l'insu des personnes concernées.

À titre illustratif, le groupe de travail de l'article 29 (dit ' G29 ' devenu le Comité européen de la protection des données (CEPD)), dans son Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, a noté à cet égard que ' les données à caractère personnel, même si elles ont été rendues publiques, restent considérées comme des données à caractère personnel ' et que ' leur traitement continue donc à requérir des garanties appropriées '. Tout en reconnaissant le fait que les données à caractère personnel soient accessibles au public peut être un facteur pertinent pour conclure à l'existence d'intérêts légitimes, le CEPD a ensuite averti que ce ne serait le cas que ' si leur publication s'accompagnait d'une attente raisonnable d'utilisation ultérieure des données à certaines fins par exemple, pour des travaux de recherche ou dans un souci de transparence et de responsabilité. '

En outre, pour que le responsable de traitement puisse se prévaloir de cette base juridique, le traitement doit être nécessaire aux fins des intérêts légitimes qu'il poursuit, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux des personnes concernées.

En l'espèce, même si l'intérêt de la société était fondé sur l'intérêt économique qu'elle tire de l'exploitation de la base de données en cause, cet intérêt devrait toutefois être mis en balance avec les intérêts ou les libertés et droits fondamentaux des personnes concernées, compte tenu des attentes raisonnables des personnes fondées sur leur relation avec le responsable du traitement, conformément à l'article 6.1.f) du RGPD, lu à la lumière du considérant 47 et de l'avis du CEPD sur la notion d'intérêt légitime précité.

En l'espèce, le traitement présente une intrusivité particulièrement forte : il recueille sur une personne donnée un grand nombre de données photographiques, auxquelles sont associées d'autres données à caractère personnel susceptibles de révéler divers aspects de la vie privée. À partir de ces données, est constitué un gabarit biométrique, c'est-à-dire une donnée biométrique permettant, si elle est fiable, d'identifier la personne de façon unique à partir d'une photographie de la personne : la détention d'une telle donnée par un tiers constitue une atteinte forte à la vie privée. Enfin, il convient de relever que ce traitement concerne un nombre extrêmement élevé de personnes.

Par ailleurs, il convient notamment de déterminer si les personnes concernées pouvaient raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un tel traitement par la société X. À cet égard, il n'existe aucune relation entre la société et les personnes concernées. Si elles peuvent raisonnablement s'attendre à ce que des tiers accèdent ponctuellement aux photographies en cause, le caractère publiquement accessible de celles-ci ne suffit pas pour considérer que les personnes concernées puissent raisonnablement s'attendre à ce que leurs images alimentent un logiciel de reconnaissance faciale. Enfin, le logiciel exploité par la société n'est pas public et la grande majorité des personnes concernées ignorent son existence.

Il doit donc être considéré que les personnes qui ont publié des photographies les représentant sur des sites web, ou consenti à cette publication auprès d'un autre responsable de traitement, ne s'attendent pas à ce que celles-ci soient réutilisées pour les finalités poursuivies par la société, c'est-à-dire la création d'un logiciel de reconnaissance faciale (qui associe l'image d'une personne à un profil contenant l'ensemble des photographies sur lesquelles elle figure, les informations que ces photographies contiennent ainsi que les sites web sur lesquels elles se trouvent) et la commercialisation de ce logiciel à des forces de l'ordre.

Dès lors, au regard de l'ensemble de ces éléments, l'atteinte portée à la vie privée des personnes apparaît disproportionnée au regard des intérêts du responsable de traitement, notamment ses intérêts commerciaux et pécuniaires, et le fondement juridique de l'intérêt légitime de la société ne peut donc être retenu.

Par conséquent, la société ne dispose d'aucune base juridique pour le traitement en cause, en méconnaissance de l'article 6 du Règlement.

Un manquement à l'obligation de respecter le droit d'accès

L'article 15 du RGPD dispose que ' la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel '. Cet article prévoit également les différentes catégories d'informations que le responsable de traitement doit fournir à la personne concernée en cas de demande d'accès.

L'article 12 précise que : ' le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22 '

En l'espèce, il ressort de la saisine n° X que la plaignante a demandé à la société l'accès aux données la concernant et à l'ensemble des informations relatives à ces données au sens de l'article 15.1, par voie électronique.

En effet, la plaignante a mandaté un tiers afin d'effectuer sa demande d'accès auprès de la société. X en a accusé réception tout en invitant la plaignante à utiliser une plateforme en ligne pour exercer sa demande. Plus de deux mois après la demande initiale et à l'issue de trois autres courriers électroniques adressés par le tiers mandaté, la société a exigé la transmission d'une photographie et d'une pièce d'identité de la plaignante et a de nouveau invité la plaignante à utiliser une plateforme en ligne pour exercer sa demande. Quatre mois après la demande initiale, après de nouveaux échanges relatifs à la transmission d'une pièce d'identité et en l'absence de réponse satisfaisante, le tiers mandaté a adressé un courrier de mise en demeure à la société.

La société a communiqué une réponse à la demande d'accès qui, tout d'abord, est partielle. En effet, celle-ci ne contient que le résultat de la recherche dans l'outil commercialisé par la société, c'est-à-dire les images et les informations qui leur sont associés. Font ainsi défaut l'ensemble des informations prévues à l'article 15.1 du RGPD, la société s'étant contentée de fournir un lien vers sa politique de confidentialité.

Ensuite, en n'acceptant de répondre à la demande d'accès de la plaignante qu'à l'issue de sept courriers et plus de quatre mois après sa demande initiale et en exigeant une copie de sa pièce d'identité alors que la plaignante avait déjà fourni des informations permettant de l'identifier ainsi qu'une photographie la représentant, X n'a pas facilité l'exercice des droits de la plaignante.

Enfin, il ressort de la politique de confidentialité de la société que celle-ci limite l'exercice du droit d'accès aux données collectées les douze mois précédant la demande et restreint l'exercice de ce droit à deux fois par an. Or, la politique de confidentialité de la société ne précise pas la durée de conservation des données et il ne ressort pas des éléments du dossier que la conservation des données en cause serait limitée à douze mois.

Il ressort de ces éléments que la société ne répond pas de manière effective aux demandes d'accès qui lui sont adressées en vertu de l'article 15 du RGPD et ne facilite pas l'exercice du droit d'accès des personnes concernées.

Ces faits constituent un manquement aux articles 12 et 15 du Règlement.

Un manquement à l'obligation de respecter le droit d'effacement

L'article 17 du RGPD prévoit : ' La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique : […] les données à caractère personnel ont fait l'objet d'un traitement illicite '.

Il ressort de la saisine n° X que la plaignante n'a reçu aucune réponse de la société concernant l'effacement de ses données qu'elle avait requis de la société.

Or, dès lors que la Commission considère que le traitement mis en œuvre ne peut reposer sur aucune base légale valide au regard de la réglementation européenne, l'effacement était de droit.

Ce fait constitue un manquement à l'article 17 du Règlement.

En conséquence, la société X, sise […], est mise en demeure sous un délai de deux (2) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

ne pas procéder sans base légale à la collecte et au traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire français dans le cadre du fonctionnement du logiciel de reconnaissance faciale qu'elle commercialise, et en particulier, supprimer l'ensemble des données à caractère personnel de ces personnes (après avoir répondu aux demandes d'accès déjà formulées le cas échéant) ;

faciliter l'exercice des droits des personnes concernées et en particulier, répondre de manière effective à la demande d'accès formulée par la plaignante en cause ;

faire droit à la demande d'effacement formulée par la plaignante en cause ;

justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

À l'issue de ce délai, si la société X s'est conformée à la présente mise en demeure, il sera considéré que la présente procédure est close et un courrier lui sera adressé en ce sens.

À l’inverse, si la société X ne s’est pas conformée à la présente mise en demeure, il est rappelé qu’un rapporteur peut être désigné pour requérir que la formation restreinte prononce l’une des sanctions prévues par l’article 20 de la loi du 6 janvier 1978 modifiée.

La Présidente

Marie-Laure DENIS