Recueil Dalloz

Recueil Dalloz 2020 p.1568

Pour un encadrement démocratique de la reconnaissance faciale

Éléments de débat

Caroline Lequesne Roth, Maître de conférences en droit public à l'Université Côte d'Azur, Responsable de la Fablex DL4T et du Master II Droit algorithmique et gouvernance des données

Face à la multiplication des usages et des inquiétudes que suscite la technologie, que dit le droit ?

Les usages et les dispositifs de la reconnaissance faciale se déclinent sur de multiples terrains. Identification des personnes d'intérêt lors d'événements publics, authentification des citoyens dans les aéroports ou des élèves dans les établissements scolaires, analyse comportementale des entretiens d'embauche ou des consultations cliniques : la technologie se déploie au service d'une inventivité humaine parfois fantasque. Si la Commission nationale de l'informatique et des libertés (CNIL) alerte quant aux risques d'atteinte « considérable » aux droits et libertés individuelles que de tels dispositifs sont susceptibles d'induire, force est de constater l'absence de législation dédiée qui en déterminerait les usages démocratiquement acceptables. Son cadre d'exploitation repose à ce jour sur le paquet législatif européen que composent le Règlement général sur la protection des données (RGPD) (2016/679, 27 avr. 2016), d'une part, la directive « Police-Justice » (2016/680, 27 avr. 2016), d'autre part. Dans leurs domaines d'application respectifs, ils établissent le principe de l'interdiction du traitement des données biométriques : celui-ci ne peut être admis sans le consentement explicite de la personne concernée ou au nom de motifs d'intérêt public important dans le cadre du RGPD (art. 9) ; il l'est « uniquement en cas de nécessité absolue » dans la directive (art. 10). En toutes hypothèses, proportionnalité et mesures de sauvegarde des droits fondamentaux et intérêts de la personne sont de rigueur. Concernant la surveillance de l'espace public, autour de laquelle se polarise aujourd'hui le débat public, la loi informatique et liberté prévoit également que le traitement des données biométriques pour le compte de l'État agissant dans l'exercice de ses prérogatives de puissance publique peut être autorisé par décret en Conseil d'État, pris après avis motivé et publié de la CNIL (art. 32).

Pourquoi l'intervention du législateur paraît-elle indispensable ?

L'intervention de ce dernier semble indispensable à divers égards. Tout d'abord, la technologie présente des failles. En sus des erreurs de correspondance encore nombreuses, les biais identifiés par plusieurs études concordantes révèlent que ces outils sont moins fiables sur les personnes de couleur, les femmes et les enfants. Concernant la reconnaissance comportementale - dont le développement est exponentiel en matière de recrutement, et qui fait l'objet de tests dans des services de transport urbain -, la communauté scientifique alerte quant à l'absence d'étude probante sur l'efficacité des technologies. Ces incertitudes ne sont pas compatibles avec leur large diffusion, susceptibles d'orienter - voire de conditionner - des décisions humaines aussi essentielles que l'arrestation d'un individu ou son accès à l'emploi. Elles le sont d'autant moins qu'elles peuvent occasionner, comme l'a souligné la CNIL, une méconnaissance des droits fondamentaux de la personne, limitée dans sa liberté d'aller et venir ou sa liberté d'expression. Le législateur se voit, en outre, « convoqué » par l'histoire, face à un choix de société qui appelle à définir les contours d'une société de surveillance.

Quelles interactions entre le régime de consentement privé et l'élaboration d'un encadrement de la surveillance « publique » ?

Tandis que les plaidoyers en faveur de l'interdiction d'un recours à la technologie dans l'espace public se multiplient, les inquiétudes entourant ses usages privés sont moins prégnantes. Seule la ville de Portland, dans l'Oregon, a proposé d'interdire le recours à la reconnaissance faciale par les entreprises. Ces dispositifs ont, de surcroît, d'ores et déjà investi notre quotidien. De l'ouverture des smartphones à l'identification des visages sur les réseaux sociaux, ces pratiques, fondées sur le consentement de chacun, ne soulèvent pas les mêmes résistances. Certes, l'hypothèse d'un contrôle en temps réel des déplacements individuels par l'État, à plus forte raison dans le cadre de manifestations politiques telles qu'à Hong Kong, Pékin ou Moscou, alimente légitimement les craintes du citoyen. Pour autant, la constitution de fichiers biométriques par les géants technologiques est tout aussi préoccupante, et les conséquences sur les vies humaines potentiellement aussi lourdes ; en témoignent l'exemple du recrutement ou la stigmatisation de certains individus dans des lieux de fréquentation privés. La dichotomie opérée méconnaît, plus fondamentalement, une réalité essentielle : celle de l'immixtion des systèmes. Les usages de la reconnaissance faciale atténuent la frontière des domaines public et privé ; ainsi a-t-on pu observer les forces de police anglaise transmettre les images de garde à vue à certains centres commerciaux pour la conduite d'expérimentations, ou l'entreprise Amazon collaborer avec la police américaine pour tester son logiciel non préalablement éprouvé.

De cette distinction résulte un double risque. Le premier en termes de légitimité : comment justifier l'encadrement étroit des usages par l'État, au nom de la sécurité nationale, quand nous consentons très largement aux usages, parfois semblables, des opérateurs privés ? Le second en termes de légalité : en admettant que les pratiques de surveillance privée sont moins dangereuses, ne court-on pas le risque de vider de leur substance les garanties offertes en matière de surveillance publique ? Si celle-ci est en partie assurée par le secteur privé, pourrons-nous admettre que le consentement constitue une frontière solide à l'autoritarisme numérique ?

Mots clés :
DROIT ET LIBERTE FONDAMENTAUX * Vie privée * Atteinte * Reconnaissance faciale * Protection
INFORMATIQUE * Nouvelle technologie * Intelligence artificielle * Reconnaissance faciale