Règlement biométrie au travail

Emmanuel Netter

Règlement biométrie au travail
commentaire par Emmanuel Netter, MCF HDR à l'Université d'Avignon

Au début de l'année 2019, la CNIL a adopté un règlement-type relatif à l'authentification biométrique au travail[1]. Son importance justifie quelques commentaires.

L'authentification biométrique a intégré la vie quotidienne. La téléphonie mobile a largement contribué, au cours des années qui viennent de s'écouler, à sa diffusion auprès du grand public. Pour déverrouiller l'appareil à l'aide des seules techniques antérieurement disponibles, par le tracé d'un modèle ou la tabulation d'un mot de passe, encore fallait-il se souvenir du sésame, puis le communiquer à la machine. L'apposition d'un doigt sur un capteur ou la présentation du visage à une caméra économisent le temps et les efforts de l'utilisateur : le sésame, c'est lui.

Rapide et pratique, l'authentification biométrique est sans doute également, dans l'esprit du grand public, particulièrement robuste. Au cinéma, lorsque le système informatique de ses adversaires est verrouillé par un classique mot de passe, le héros sera toujours en mesure de le deviner en moins de dix tentatives, en combinant habilement l'année de naissance de l'utilisateur avec le nom de son animal de compagnie. Inversement, si l'entrée dans un système ou des locaux est subordonnée à un test biométrique, le spectateur sait que débute une longue séquence, qui s'achèvera vraisemblablement par l'enlèvement de l'antagoniste et sa présentation forcée devant les capteurs. La réalité est plus nuancée. Il y a moins d'empreintes digitales possibles, par exemple, que de mots de passe longs, ce qui facilite les attaques de certains systèmes biométriques par force brute[2]. Il est plus facile de recueillir une empreinte digitale laissée sur un verre au restaurant que d'amener un subordonné loyal à dévoiler une chaîne de caractères secrète[3]. En revanche, une bonne identification biométrique vaut certainement mieux qu'un mot de passe court et prévisible, ou écrit sur un post-it collé à un écran d'ordinateur. Tout dépend donc du « modèle de menaces » contre lequel on entend prioritairement se prémunir. Par ailleurs, les systèmes biométriques sont loin de présenter une robustesse uniforme : de leur type, de leur qualité – et donc de leur coût – dépend la sécurité qu'ils sont en mesure d'offrir.

L'authentification biométrique a quoi qu'il en soit pour elle son caractère rapide et indolore, qui en fait un choix séduisant pour qui doit s'y soumettre des dizaines de fois par jour : l'utilisateur de téléphone qui souhaite – à juste titre – le verrouiller à chaque fois qu'il cesse de l'utiliser, ou le salarié d'un site sécurisé amener à franchir sans cesse les limites d'une zone à restriction d'accès.

Il est toutefois un inconvénient propre aux techniques biométriques sur lequel insiste la CNIL : « Si un mot de passe a été divulgué, il est possible de le renouveler. En revanche, il est impossible de changer son empreinte digitale, qui est un élément du corps humain »[4]. L'affirmation se transpose évidemment aux caractéristiques du visage ou du réseau veineux de la main. Dans un monde où l'authentification et l'identification biométriques sont partout, que devient celui dont les

1 Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail.

2 Le taux de « faux positifs » sur la technologie d'authentification par empreintes digitales d'Apple était évalué, par le fabricant, à 1 sur 50 000, ce qui n'est pas négligeable. La reconnaissance du visage est présentée comme plus performante : https://www.lci.fr/high-tech/iphone-x-apple-veut-rassurer-sur-face-id-2065771.html.

3 Sur l'attaque consistant, ensuite, à fabriquer un « faux doigt » pour le présenter au capteur : CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, p. 4.

4 CNIL, communication précitée relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale… p. 5.

caractéristiques physiques sont connues et reproductibles à volonté par une entité malveillante[5] ? Le danger n'est pas théorique, comme l'a confirmé une affaire récente[6].

Ces risques extraordinairement élevés expliquent que le RGPD intègre « les données biométriques aux fins d'identifier une personne physique de manière unique » parmi les données sensibles de l'article 9, qui font l'objet d'une interdiction de traitement de principe, assortie toutefois de plusieurs exceptions. Le point 4 du même article laisse aux États membres une importante marge de manœuvre, qui leur permet de fixer des règles plus précises en la matière. Voici qui invite à se tourner vers le droit interne : la loi informatique et libertés prévoit que « Les traitements (...) mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires », mais à condition qu'ils soient conformes à un règlement-type de l'autorité de contrôle[7]. C'est précisément ce règlement que la CNIL a adopté en janvier dernier.

L'autorité s'était déjà intéressée à ces questions bien avant l'entrée en application du RGPD. Sous l'empire de l'ancien système, on sait que les responsables de traitement devaient se plier à des « formalités préalables » qui allaient, dans les domaines les plus sensibles, jusqu'à la nécessité de recueillir une autorisation *a priori* de la CNIL. Mais une « autorisation unique » avait été délivrée pour les authentifications biométriques au travail obéissant à certains critères stricts[8]. Les traitements qui en différaient restaient soumis à l'exigence d'une autorisation au cas par cas. Aujourd'hui, les formalités préalables ont disparu, et il n'est plus question d'autorisations individuelles ni collectives. Le texte que vient de produire la CNIL n'est par conséquent plus un simple coupe-file dispensant seulement d'un examen personnel de situation : il est une réglementation directe, obligatoire et exhaustive de la question. Si le règlement-type diffère donc clairement de l'autorisation unique de par sa nature juridique, les deux textes reposent sur les mêmes concepts-clés. Ils attachent en particulier une grande importance à la question de savoir qui, du salarié ou de l'employeur, a la maîtrise matérielle du fichier contenant la caractéristique biométrique numérisée. Mais n'anticipons pas, et examinons le texte dans l'ordre.

Les deux premiers articles sont relatifs au champ d'application du règlement et aux finalités de traitement concernées. Sont visées par ce texte les authentifications biométriques barrant l'accès à des appareils ou à des locaux, dans le cadre d'une relation de travail, peu important que l'employeur soit une personne publique ou privée. Restent donc hors du champ du texte, par exemple, les expériences récentes de reconnaissance du visage à l'entrée de lycées – les élèves n'étant pas des employés. C'est alors le droit commun des données personnelles qui s'appliquera.

On rencontre ensuite la définition d'une notion centrale du texte, celle de « gabarit » (en anglais, *template*) : il s'agit du « résultat du traitement de l'enregistrement brut (photo, enregistrement audio, etc.) de la caractéristique biométrique par un algorithme rendant impossible la reconstitution de celle-ci ». Ce que manipuleront les systèmes chargés d'autoriser ou non les accès, ce sont des

5 L'authentification consiste, pour une personne préalablement enregistrée dans un système (par exemple le salarié d'une entreprise) à prouver qu'elle est bien celle qu'elle prétend. L'identification consiste à relier une personne inconnue à une identité. C'est ce qui se produit par exemple lorsqu'un système public de vidéosurveillance appose des noms sur les citoyens qui se promènent dans la rue filmée. Sur cette distinction, V. par ex. les explications de Gemalto : https://www.gemalto.com/france/gouv/inspiration/biometrie.

6 L. Collart, « Une faille de sécurité expose des empreintes digitales de 2000 belges », article lesoir.be du 20 août 2019. Heureusement, le défaut a été signalé par des chercheurs en sécurité bienveillants, et la faille a été comblée.

7 Art. 44, 4° de la loi n° 78-17 du 6 janvier 1978. Le pouvoir globalement reconnu à la CNIL d'édicter des règlements-types est par ailleurs abordé à l'art ; 8 c) du même texte.

8 Délibération n° 2016-186 du 30 juin 2016 portant autorisation unique de mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail et garantissant la maîtrise par la personne concernée sur son gabarit biométrique (AU-052)

images transformées des caractéristiques physiques. L'assaillant qui parviendrait à piller une base de gabarits n'y trouverait pas les photographies pures et simples des iris ou des empreintes papillaires des salariés, mais seulement des informations dérivées. Remonter à la caractéristique physique serait alors difficile – mais pas impossible. L'article premier rappelle enfin que le règlement-type ne fait qu'appliquer à un domaine précis certaines obligations générales découlant de la loi informatique et libertés et du RGPD, mais qu'il ne se substitue pas à ces textes pour le surplus.

Cette idée selon laquelle le règlement ne fait, pour l'essentiel, que mettre en musique les concepts fondamentaux du RGPD, s'illustre très bien avec les articles suivants, qui constituent des applications particulières du principe de minimisation (art. 5, 1, c RGPD).

Article 3. Le responsable de traitement devra documenter les raisons pour lesquelles il est « nécessaire » (et non simplement expédient) de recourir à la biométrie, plutôt qu'à un procédé de contrôle des accès moins menaçant pour la vie privée des personnes concernées, comme des badges ou des mots de passe. Selon le degré de rigueur avec laquelle elle sera appliquée, cette règle peut se révéler redoutable. Dans un monde où les salariés appliquent avec rigueur une politique de mots de passe forts, les saisissent avec patience cinquante fois dans la journée s'il le faut, ne perdent jamais leurs badges, dans un univers où les services de sécurité sont bien dimensionnés en personnel et correctement formés, la biométrie ne sera que très rarement nécessaire. Ce monde, toutefois, n'existe pas, et la CNIL le sait. L'essentiel, pour le responsable de traitement, est de documenter son choix avec le plus grand sérieux.

L'article 4 présente une liste strictement limitative des données susceptibles d'être traitées dans le cadre du règlement. Elles ont trait pour l'essentiel à l'identité de la personne contrôlée (nom ou matricule, gabarit), à sa situation dans l'entreprise, aux matériels et locaux auxquels un accès lui est attribué.

L'article 5 rappelle qu'il existe différents modes d'authentification biométriques, mais qu'ils ne sont absolument pas fongibles. D'abord, le recours à certains d'entre eux est tout simplement interdit : ceux qui nécessitent le prélèvement d'un produit humain, comme le sang ou la salive. Ensuite, parmi ceux qui subsistent, le responsable de traitement devra documenter les raisons qui l'ont fait choisir, par exemple, une reconnaissance du réseau veineux de la main plutôt que des empreintes digitales. Les caractéristiques qui guideront le responsable de traitement sont certainement la robustesse de la technologie (par exemple, le taux de faux positifs ou négatifs, dont le caractère acceptable varie fortement selon le contexte) et, naturellement, son coût. Il faudrait les mettre en balance avec le caractère intrusif de la technique. Cela suppose qu'il ne soit pas toujours le même. Il nous semble que le recours au réseau veineux de la main, par exemple, est moins sensible que le recours aux empreintes digitales, tant ce dernier est répandu aussi bien en matière de documents d'identité que d'usages domestiques, de sorte qu'une « fuite » de données aura de plus grandes conséquences. A suivre ce raisonnement, l'identification faciale est plus sensible encore : qu'un gabarit de son visage circule, et l'individu pourra être identifié par des moyens automatisés sur toute photographie ou vidéo sur laquelle il sera présent.

L'article 6 applique oblige à minimiser les personnes ayant accès aux données, selon la catégorie d'informations considérée. Par exemple, les informations biométriques elles-mêmes seront gérées par un service spécialisé, composé d'un petit nombre de personnes habilitées. Les données générées par le dispositif (par exemple, un journal des accès à un local sensible) seront accessibles à une autre catégorie de personnel, celle des responsables de la sécurité.

L'article 7 doit retenir l'attention. Il distingue trois grandes techniques de gestion du gabarit. Le « type 1 » renvoie aux gabarits « sous la maîtrise des personnes concernées » : ils sont stockés exclusivement sur un support détenu par la personne concernée, par exemple un badge. Le « type

2 », celui des « gabarits sous maîtrise partagée », fait usage d'une base centrale dans laquelle sont stockées les images des caractéristiques biométriques. Toutefois, les gabarits sont chiffrés, et le secret permettant de les faire apparaître en clair est aux mains de la personne concernée et d'elle seule. Il peut s'agir d'un code PIN, d'un mot de passe, d'une clé de chiffrement stockée sur un support mobile… La solution 2 apparaît à l'évidence comme plus dangereuse, car la base centrale constitue une cible de choix pour des assaillants. Mais puisqu'elle est théoriquement inexploitable sans les secrets aux mains des employés, le risque reste limité. Dans le « type 3 », il existe une base centrale, et celle-ci peut être déchiffrée sans l'apport d'un secret aux mains des employés : le danger est donc à son maximum.

Le règlement ne fait une nouvelle fois que tirer les conséquences du principe de minimisation, quand il exige que l'on retienne le type le moins intrusif possible au regard du contexte et que l'on documente la solution choisie. Le type 1 semble envisageable dans l'écrasante majorité des cas. Idéalement, le test de concordance entre la caractéristique physique présentée par l'employé et son enregistrement numérique a lieu directement sur le badge dont il est porteur (système « match-on-card »), et la carte ne fait que renvoyer à l'employeur le résultat du test, positif ou négatif. Le gabarit ne transite pas au cours de l'opération, et la protection est donc maximale. Dans quel cas pourra-t-on justifier de recourir à un type 2, voire 3 ? Dans ses « questions-réponses » autour du règlement, la CNIL évoque par exemple des situations dans lesquelles le port d'un badge pourrait compromettre la stérilité d'un bloc opératoire, d'une chaîne de production alimentaire ou d'une salle blanche de production de microprocesseurs : il s'agit bien de cas de figure strictement limités[9].

L'article 8 est le dernier étage de la fusée « minimisation » et porte sur les durées de conservation. Relevons notamment que l'enregistrement brut de la caractéristique biométrique (par exemple la photographie d'une empreinte ou d'un iris) ne peut servir qu'au calcul en temps réel du gabarit, et ne fait l'objet d'aucune conservation. Seuls les gabarits sont conservés, mais ils sont eux-mêmes supprimés immédiatement lorsque cessent les fonctions de l'employé.

L'article 9 constitue un pur et simple rappel des obligations de transparence issues des articles 12 et suivants du RGPD, qui conduiront notamment à remettre aux personnes concernées des informations écrites sur les grandes caractéristiques du traitement.

L'article 10 est plus intéressant, car il ne se contente pas de rappeler la substance de l'article 32 du RGPD, selon lequel des mesures techniques et organisationnelles adéquates doivent être prises pour assurer la sécurité du traitement : il fixe une longue liste de mesures concrètes dont l'adoption constitue le minimum attendu de la part du responsable de traitement. Ces directives s'adressent davantage aux responsables des systèmes d'information qu'aux juristes, c'est pourquoi nous n'entrerons pas dans leur détail. Il s'agit de mesures relatives aux données (par exemple, utiliser un algorithme de hachage pour vérifier que les informations n'ont pas été altérées volontairement ou par accident ; veiller à détecter les tentatives de fraude comme l'utilisation de « faux doigts »…), à l'organisation (toujours prévoir une alternative de secours à l'identification biométrique, pour les personnes ne pouvant s'y soumettre en raison de leurs caractéristiques physiques ou en cas de panne…), aux matériels, aux logiciels et aux canaux informatiques employés.

Enfin, **l'article 11** est relatif aux analyses d'impact. Rappelons qu'aux termes de l'article 35 du RGPD, « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, **est susceptible d'engendrer un risque élevé** pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ». Les autorités de contrôle nationales peuvent établir des listes de traitement dont il est irréfragablement présumé qu'ils

9 https://www.cnil.fr/fr/question-reponses-sur-le-reglement-type-biometrie.

engendrent un risque élevé pour les droits et libertés des personnes[10]. La CNIL décide, à l'occasion du règlement rapporté, que les traitements qu'il régit donnent obligatoirement lieu à une analyse d'impact. Elle précise que « le choix de recourir aux modalités de détention du gabarit biométrique garantissant une moindre maîtrise de la personne, en particulier du type 3, doit faire l'objet d'une documentation particulièrement circonstanciée ».

En vertu du droit commun des données personnelles si, à l'issue de l'analyse d'impact, un risque élevé subsiste pour les droits des personnes concernées, une consultation de l'autorité de contrôle est obligatoire avant tout démarrage du traitement (art. 36, 1 RGPD), ce qui constitue un quasi-retour à une logique de formalités préalables. La faiblesse de ce système, c'est que le responsable de traitement peut sous-estimer (volontairement ou non) la dangerosité des opérations qu'il s'apprête à lancer, et s'abstenir alors de consulter l'autorité. Or, il nous semble que les traitements de types 2 et 3 sont à la fois si dangereux et si difficiles à justifier au regard des critères du règlement, qu'il aurait été souhaitable qu'ils fassent toujours l'objet d'un examen préalable et au cas par cas. Certes, rien dans le RGPD ne semble autoriser à ce que l'on présume certaines analyses d'impact, de manière irréfragable, comme laissant subsister à leur terme un risque élevé pour les libertés des personnes concernées. Mais une approche technique encore plus directe semble envisageable, laissant derrière elle la question des analyses d'impact : si un pouvoir réglementaire est reconnu à la CNIL d'autoriser et d'interdire certains types d'authentification biométrique, on ne voit pas pourquoi on lui refuserait la possibilité d'autoriser certains traitement sous condition d'examen individuel préalable : qui peut le plus peut le moins. À supposer que cette analyse soit considérée comme contraire aux textes, *de lege lata*, il conviendrait alors de les modifier en ce sens.

10 Pour la CNIL, V. la délibération n° 2018-327 du 11 octobre 2018.