CRSI
CENTRE DE RÉFLEXION
SUR LA SÉCURITÉ INTÉRIEURE

NOTE FLASH
Janvier 2022

Pour un usage augmenté de la biométrie au service d'une meilleure sécurité publique

Benoit Fayet
Consultant en transformation numérique
Membre du comité stratégique du CRSI

Les événements sportifs mondiaux à venir en France en 2023 (Coupe du Monde de rugby) et 2024 (Jeux Olympiques et Paralympiques) sont une formidable perspective pour notre pays, **mais représentent également une menace majeure en termes de sécurité publique.** L'amélioration des capacités de contrôle et de vérification des identités à grande échelle, la mise à disposition de bases de données plus fiables et l'usage de technologies adaptées pour les forces de sécurité intérieure sont, entre autres, des enjeux clés pour être en mesure de répondre aux attentes liées à l'organisation future de ces évènements mondiaux. Au-delà de ces évènements, la situation sécuritaire fortement dégradée en France aujourd'hui (terrorisme, violences et insécurité au quotidien, crise migratoire…) appelle **à identifier des solutions capables d'apporter sur le long terme des réponses pour assurer la sécurité des citoyens.**

Parmi ces solutions, l'usage des biométries au service de la sécurité publique doit être débattu. Les échéances électorales à venir cette année doivent être le cadre de ce débat fondamental et, en amont, des échéances mondiales précitées, pour **améliorer la sécurité des français de manière durable tout en ne transigeant pas sur la protection des données et leur bon usage, qui sont autant de principes fondamentaux de notre société.**

Biométrie, biométries ? Quel cadre juridique ?

La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques ou biologiques. La biométrie évolue aujourd'hui au-delà des techniques « historiques » (biométrie faciale, digitale ou génétique) avec d'autres techniques émergentes (biométrie comportementale, olfactive, vocale…) présentant des maturités techniques et technologiques différentes, faisant que l'on parle désormais des biométries ou de la multi-biométrie. **La reconnaissance biométrique de l'individu se fait par identification ou par authentification.** L'identification consiste à repérer un individu dans un espace et une population donnés à partir de ce qui est déjà connu de lui d'un point de vue biométrique; l'authentification consiste à confronter des données biométriques déjà enregistrées à celles présentées par un individu lors d'un contrôle.

Les données biométriques sont des données à caractère personnel, car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (empreintes digitales, ADN…). À ce titre, les données biométriques ont légitimement un cadre juridique strict et sont classées dans la catégorie des données sensibles au sens de la loi « Informatique et Libertés » et du RGPD[1]. Le RGPD interdit le traitement des données biométriques aux fins d'identifier une personne physique de manière unique, mais des exemptions sont prévues quand la personne concernée a consenti au traitement de ses données, lorsque le traitement porte sur des données rendues publiques par cette personne ou pour des motifs d'intérêt public. Ce cadre juridique a été complété dernièrement par la Directive « Police-Justice », qui autorise le traitement des données biométriques aux fins d'identifier une personne physique de manière unique seulement en cas de nécessité absolue et sous réserve de garanties appropriées pour les droits et libertés de la personne concernée.

Quels usages aujourd'hui de la biométrie par les forces de sécurité intérieure ?

La biométrie est depuis longtemps utilisée par les policiers nationaux ou les gendarmes au quotidien, et constitue **un outil indispensable et**

[1] Règlement européen relatif à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

essentiel d'un point de vue opérationnel dans leurs missions d'enquête, de recherche d'auteurs d'infractions et de matérialisation de la preuve, de surveillance et de contrôle du territoire qui, par la nature même de ces missions, nécessitent de reconnaître l'identité des personnes. La biométrie est devenue indispensable notamment pour les activités de lutte contre la fraude et l'usurpation d'identité par rapport aux moyens existants liés à la donnée alphanumérique. Des fichiers informatiques[2] ont été créés permettant, dans l'exercice de ces missions de sécurité intérieure, de collecter des données biométriques digitales ou génétiques et de procéder à une signalisation biométrique de personnes ayant commis des infractions.

« Il convient de dépasser les débats actuels autour de la biométrie via des expérimentations concrètes »

D'autres fichiers informatiques disposent également de données biométriques, comme le TAJ[3] par exemple, où figurent des images faciales de certaines personnes qui y sont inscrites. En outre, de récents règlements européens visant à renforcer le contrôle aux frontières extérieures de l'UE et la coopération policière entre les pays membres de l'accord de Schengen prévoit que des données biométriques (photographies, empreintes digitales) figurent à terme dans les fichiers nationaux de ces pays, qui pourraient alors être interrogés sur ces données en cas de signalement. Une mise en conformité de la France à ces règlements est en cours.

Quels usages demain de la biométrie par les forces de sécurité intérieure ?

Au-delà de ces usages existants, les nouvelles potentialités technologiques actuelles autour de la biométrie doivent être étudiées pour permettre aux forces de sécurité intérieure d'être plus performantes dans leurs missions de sécurité publique, de police judiciaire, de renseignement ou de contrôle aux frontières. Il apparaît que la Coupe du Monde de rugby en 2023 et les Jeux Olympiques et Paralympiques de 2024 sont **une opportunité pour tester en situation réelle ces nouveaux usages dans un cadre expérimental juridiquement strict,** avant d'éventuellement les généraliser ensuite au-delà de ces évènements, si ces usages sont concluants et respectent la protection des données personnelles. Il semble notamment que la Coupe du Monde de Rugby, évènement de moindre ampleur, pourrait être le cadre d'expérimentations réunissant l'ensemble des acteurs concernés, juridiques, opérationnels (policiers nationaux et gendarmes) et politique.

Il convient en effet de dépasser les débats actuels via des expérimentations concrètes, pour s'assurer que les technologies répondent aux besoins opérationnels des forces de sécurité intérieure, définir précisément avec les acteurs juridiques concernés les cas d'usage, l'analyse d'impact relative à la protection des données personnelles, construire le cadre de contrôle et d'évaluation nécessaire et enfin tester et démontrer la maturité technique de technologies qui seront alors meilleures et mieux maîtrisées une fois ces expérimentations réalisées. **Seuls des tests en situation réelle menés en France permettront en outre de développer des technologies de confiance en lien avec l'écosystème industriel national.**

La distinction entre authentification et identification biométrique évoquée plus haut est structurante pour maintenir un niveau acceptable juridiquement de l'usage de la biométrie au service de la sécurité publique. L'identification biométrique n'apporte pas de garantie à date, à ce titre, en termes de fiabilité technologique et donc d'un point de vue juridique. **Il apparaît donc que le recours à l'authentification biométrique soit plus acceptable juridiquement et plus fiable technologiquement à ce jour** et que cela puisse être, lors des événements sportifs de 2023 et 2024, une solution à expérimenter. L'authentification biométrique pourrait ainsi être testée pour accéder à des sites lors de la Coupe du Monde de rugby et les Jeux Olympiques et Paralympiques (stades, fans zones, village olympique, centres d'entraînement). Une fois l'analyse d'impact relative à la protection des données personnelles réalisée, si le cadre technologique et les gains opérationnels sont réels, une extension à des cas d'usage ultérieurs pourrait alors être envisagée, comme l'authentification biométrique pour des accès à des sites sensibles (sites touristiques ou culturels par exemple), qui nécessitent un ticket où les personnes se sont déjà authentifiées pour accéder à ces sites. En termes d'authentification, la biométrie digitale ou faciale peut ainsi renforcer les dispositifs d'authentification aux points d'accès à des sites sensibles. Elle fiabilise le processus de contrôle qui repose aujourd'hui essentiellement sur des cartes ou des titres d'identité dont l'utilisation peut être facilement usurpée. Le but recherché est la lutte contre les risques d'intrusions par usurpation d'identité ou de badges dans des sites réunissant du public. Ces authentifications pourraient se faire sur le modèle du dispositif de contrôle aux frontières PARAFE, sans stockage centralisé de

[2] Fichier automatisé des empreintes digitales (FAED) et Fichier national automatisé des empreintes génétiques (FNAEG).
[3] Traitement des Antécédents Judiciaires.

données à caractère personnel et sans recours à une base de données biométriques pour comparer des données.

L'authentification biométrique est aussi un levier intéressant pour servir ensuite dans d'autres cadres, comme les transports en commun, gares ou stations de métro pour repérer des individus recherchés sur la base de listes de personnes préalablement définies *(watchlists)* encadrées juridiquement et issues de fichiers informatiques du type FPR[4], ce qui permet de limiter l'impact en termes de protection des données et de ne pas opérer une surveillance indifférenciée de l'ensemble des personnes présentes dans une station ou une gare.

Dans ce cas d'usage (temps réel dans l'espace public), l'un des principaux termes du débat porte sur les données d'entrée à insérer dans le dispositif, l'expérimentation reposant en effet sur des listes de personnes recherchées suivant des critères définis en amont. L'utilisation de watchlists issues de fichiers informatiques supposerait un travail en amont d'analyse d'impact en termes de protection des données personnelles, du fait de l'utilisation d'une partie des données de ces fichiers informatiques, au regard du principe de proportionnalité défendue par la CNIL et devrait naturellement faire l'objet d'une autorisation par la loi ou par décret.

« La biométrie, un levier pour renforcer la sécurité des Français, tout en garantissant la protection des données personnelles »

L'authentification biométrique peut aussi permettre de **rechercher dans un espace donné une personne prédéfinie via la reconnaissance faciale.** Il est techniquement possible de localiser dans un espace défini ou parmi une foule définie des personnes recherchées pour une infraction, via un scan avec les concordances possibles avec des fichiers préalablement autorisés à être consultés juridiquement. Il n'est donc pas nécessaire d'identifier l'ensemble des personnes présentes dans l'espace et qui n'offrent pas de correspondance avec la base de recherche. Cette technologie peut également se limiter à des cas d'usage spécifiques, que ce soit la recherche d'une personne jugée dangereuse dans une zone où elle aurait été repérée, à des fins de prévention ou de poursuite, ou la recherche d'une personne disparue en danger ou identifiée comme victime.

L'analyse pourrait se faire à terme sans reconnaissance faciales via d'autres biométries, comme la biométrie comportementale. Expérimenter en situation réelle la biométrie comportementale lors de la Coupe du Monde de rugby et les Jeux Olympiques et Paralympiques est **une piste intéressante pour faciliter l'identification des situations de danger et détecter automatiquement des anomalies dans un espace donné et bien délimité**, via le déploiement de scanners corporels par exemple. Il s'agit de solutions qui pourraient être testées puis étendues à terme, au-delà de ces évènements qui sont une occasion unique de tester en situation réelle une approche multi-biométrique et tenir compte de l'émergence des biométries dites « à distance » (visage, voix, odeur). Les biométries à distance sont capables de repérer des situations anormales et de donner l'alerte notamment d'intrusions, de franchissements massifs, de colis suspects ou encore de bagarres ou agressions. Les résultats des expérimentations réalisées jusqu'alors ne semblent pas concluants, aussi la Coupe du Monde de rugby et les Jeux Olympiques et Paralympiques à venir doivent être l'opportunité de tester à nouveau ces dispositifs pour, s'ils sont concluants juridiquement (après analyse d'impact relative à la protection des données personnelles), technologiquement et opérationnellement, les étendre à des cas d'usage ultérieurs. Les biométries à distance peuvent en outre optimiser le visionnage des caméras de vidéoprotection ou des caméras embarquées (véhicules) ou piétons. L'analyse automatisée a posteriori rend possible un traitement d'images en grande quantité, qui aurait été difficile ou impossible pour des opérateurs humains.

Enfin, une autre opportunité liée à la biométrie concerne la **modernisation des équipements mobiles des forces de sécurité intérieure**. En lien avec l'authentification biométrique, l'idée serait de développer des solutions de captation biométrique adaptées aux smartphones utilisés par les policiers nationaux et les gendarmes au quotidien dans le cadre de leurs missions de sécurité publique ou de police judiciaire[5], pour authentifier un individu en temps réel aux abords d'un site sensible ou en amont d'un évènement via des capteurs d'empreintes digitales sans contact ou de la biométrie du visage via la caméra d'un smartphone. Ces solutions sans contact répondant en outre aux enjeux sanitaires actuels. Les technologies de captation biométrique déportées sur smartphone existent et sont disponibles. Il peut être opportun de les tester à grande échelle

[4] Fichier des personnes recherchées (FPR).
[5] Terminaux NEO.

lors de la Coupe du Monde de rugby et les Jeux Olympiques et Paralympiques à venir.

Le développement de modules techniques d'interrogation des fichiers informatiques (TAJ…) depuis un smartphone à partir de la captation numérique d'une empreinte digitale peut aussi être une piste de réflexion et une solution à tester, spécifiquement pour les opérations de vérification d'identité ou d'investigation judiciaire qui le justifient. Naturellement, une analyse d'impact juridique devrait être effectuée au préalable pour cela, sachant que le recueil d'empreinte digitale dans le cadre d'une vérification d'identité est une possibilité désormais offerte par de récents règlements européens[6].

En conclusion, au regard de la situation sécuritaire très dégradée aujourd'hui en France, **il semble indispensable d'envisager des moyens nécessaires à un renforcement de la protection des Français**. Les prochains évènements sportifs mondiaux à venir en France doivent être ainsi l'opportunité de tester en situation réelle de nouveaux usages des biométries au service d'une meilleure sécurité publique. Cet usage de technologies ne doit pas être une fin en soi mais un levier supplémentaire pour renforcer à long terme la sécurité des Français au-delà de ces évènements, tout en garantissant la protection des données personnelles et leur bon usage, qui sont autant de principes fondamentaux de notre société, ce que peuvent permettre des expérimentations en amont puis en situation réelle. ■

[6] Règlement (UE) n° 2018/1862 relatif au Système d'information Schengen.