

Réforme de l'échange des données policières en Europe : vers une surveillance renforcée ?

Publié: 16 mai 2022, 21:47 CEST

Yoann Nabat

Doctorant en droit privé et sciences criminelles, Université de Bordeaux



Le risque est celui d'une massification de la surveillance en autorisant l'accès systématique à toutes les bases de données policières européennes, y compris aux informations les plus sensibles (données génétiques et photographies) et par les mécanismes les plus automatisés (comparaisons informatisées, reconnaissance faciale, etc.). Fred Tanneau/AFP

Pandémie, soutien à l'Ukraine, politiques économiques : plus que jamais, l'Union européenne semble au-devant de nombreuses actualités. Parmi les objectifs assignés à l'Union européenne se trouvent bien sûr des enjeux économiques, démocratiques et sociétaux mais également sécuritaires. L'Union doit ainsi permettre de favoriser une plus grande sécurité au sein de l'espace européen.

Or, répondre à cet impératif implique notamment de favoriser la coopération entre les organes policiers et judiciaires de chaque pays. En ce sens, on a récemment évoqué la création d'un parquet européen qui doit devenir une autorité de poursuite centralisée pour certaines infractions.

Peut-être moins médiatique se trouve ici la question de l'échange des informations entre services de pays différents. Elle apparaît pourtant absolument essentielle dans la pratique quotidienne des forces de l'ordre et des juridictions, de l'enquête au jugement.

Des traités existants

C'est pour ces raisons que dans le cadre des accords de Schengen, assurant la libre circulation des personnes entre les pays signataires, a été mis en place un système policier d'échange d'informations. Le Système d'information Schengen (SIS), désormais dans sa seconde version, constitue ainsi toujours la principale source de renseignements pour les enquêteurs lors d'infractions transfrontalières.

Le SIS est une grande base de données. Organisé en plusieurs fichiers, il contient des informations notamment sur des personnes recherchées et sous surveillance policière. Il comprend un grand nombre de données, y compris les empreintes digitales. Néanmoins, son usage est très encadré et passe notamment par un bureau national présent dans chaque pays. Par ailleurs, le SIS ne permet pas l'échange des informations génétiques.

Pour répondre à ces marques, le traité de Prüm (appelé par certains « Schengen plus ») a été signé en 2005 d'abord pris entre quelques États. Intégré au droit de l'Union européenne en 2008, il autorise ainsi l'échange automatisé entre les services de police des différents pays européens des empreintes digitales mais aussi notamment des données génétiques et des informations portant sur l'immatriculation des véhicules.

Ces communications entre polices européennes peuvent avoir lieu sur tout type de délit ou de crime, mais sont sans doute en pratique le plus souvent réservées aux cas de criminalité transfrontalière (comme un trafic de stupéfiants par exemple).

Un cadre jugé insuffisant

C'est du système de Prüm, qui existe toujours en parallèle du SIS, dont on reparle aujourd'hui. En effet, plus de quinze ans après, voilà plusieurs mois que les Européens échangent à nouveau sur ces questions pour permettre l'adoption d'accords « Prüm 2 ».

La présidence française du Conseil de l'Union européenne, si elle n'est pas à l'initiative du projet, y prend une part importante et appuie sa finalisation.

Pourquoi une telle nécessité ? Dans un document de décembre dernier, la Commission européenne expose ce que serait le tableau noir des échanges policiers dans le cadre actuel : accords partiels, multiples et complexes, équipements non compatibles, pas de canal unique de communication, pertes d'informations.

Plus encore, un manque se ferait ressentir dans la pratique, selon le même document : l'absence d'outil automatisé de comparaison des images faciales des personnes fichées. Si les photographies peuvent déjà être échangées, cela se fait au cas par cas, de manière manuelle, ce qui engendrerait une perte de temps importante.

Deux modifications majeures

Le nouveau système proposé doit répondre à ces critiques. Pour cela, deux modifications majeures sont proposées.

D'une part, en lieu et place du cadre actuel qui fonctionne par échanges bilatéraux, comme une messagerie électronique, le projet d'accord prévoit un système centralisé. Il ne s'agirait donc plus, par exemple, pour le policier français de demander au policier espagnol une information sur un suspect, qui lui répond, de manière manuelle ou automatisée. Désormais, le policier français se connecterait sur une interface centralisée lui donnant directement accès aux différentes bases nationales qui y seraient toutes connectées.

D'autre part, le nouveau système permettrait l'échange de photographies faciales, pour le moment exclues du dispositif. L'usage de systèmes de reconnaissance faciale à partir de ces banques de données serait également permis. Les casiers judiciaires seraient également accessibles automatiquement.

Un avis mitigé de la CNIL européenne

Ces modifications ne sont pas mineures mais relèvent en réalité d'un changement d'échelle. En effet, même si cette réforme ne conduit pas à la création d'une base de données centralisée, elle permet une recherche automatisée et immédiate dans tous les fichiers nationaux des pays membres.

Des garde-fous encadrent bien sûr cette possibilité. Le texte prévoit ainsi que, en cas d'usage du système de reconnaissance faciale, le « match » ne pourra être validé que par un humain qui devra confirmer l'identité de la personne.

À lire aussi : Vidéo-surveillance : où vont nos données ?

Pour autant, les risques sur les libertés fondamentales et, partant, en matière de surveillance, sont réels. Le CEPD, autorité européenne de la protection des données (sorte de CNIL européenne) a ainsi très récemment mis en garde, dans son avis rendu sur le projet dans sa dernière version, sur plusieurs points importants.

Le CEPD soulève ainsi notamment l'absence de nécessité de démontrer des soupçons d'un crime grave sur un individu pour pouvoir procéder à la recherche dans les bases européennes. Les infractions autorisant cette consultation ne sont même pas précisément délimitées. Le risque est alors celui de consultations assez régulières voire massives, même en dehors de caractère particulièrement grave ou transfrontalier.

Le menace d'une massification de la surveillance

En ce sens, la recherche automatisée par données génétiques est possible quelque soit l'infraction et quel que soit le statut de la personne fichée. En France, le FNAEG autorise ainsi la collecte de personnes seulement soupçonnées, sans même qu'elles n'aient été condamnées. Le projet « Prüm 2 » ne distingue pas et prend en compte l'ensemble de ces informations.

Ces deux dernières remarques font peser le risque d'une surveillance massifiée. Cela d'autant plus que l'usage de la reconnaissance faciale à l'échelle européenne serait grandement facilité par cet accord, alors même que les critiques contre cette technologie sont nombreuses, y compris au niveau européen. Celle-ci permet en effet un contrôle d'identité virtuel permanent des individus sur l'espace public, sans compter les risques de discrimination de certaines populations.

Plus encore, même s'il est précisé que l'obtention des informations ne pourra se faire qu'en accord avec le droit national de l'agent demandeur, des questions pourraient en outre être soulevées quant au cadre français. Par exemple, en France, les policiers n'ont pas directement accès au casier judiciaire que peut seul consulter un magistrat alors même qu'il serait ici permis l'échange automatique des casiers entre services policiers.

Concrètement, le risque est donc bien celui d'une massification de la surveillance en autorisant l'accès systématique à toutes les bases de données policières européennes, y compris aux informations les plus sensibles (données génétiques et photographies) et par les mécanismes les plus automatisés (comparaisons informatisées, reconnaissance faciale, etc.).

Ainsi, derrière ces considérations qui pourraient paraître particulièrement techniques, c'est bien à travers le prisme de la surveillance et du respect des libertés fondamentales qu'il faut étudier ce projet. Celui-ci s'inscrit d'ailleurs dans un contexte général, tant européen que national, où la future Loi de programmation et d'orientation du ministère de l'Intérieur favorise encore la vidéosurveillance et l'accès aux bases de données.