

## L'interconnexion des fichiers de police : au service ou au détriment des droits fondamentaux ?

**Yoann Nabat** (droit, philosophie du droit, criminologie)

À l'origine de la loi *Informatique et Libertés* et de la naissance de l'autorité de contrôle désormais connue de tous chargée de la faire appliquer, la CNIL, se trouvait un projet gouvernemental d'interconnexion massive des fichiers détenus par l'État appelé projet *SAFARI*<sup>1</sup>. Le scandale de l'époque se nichait précisément dans l'interconnexion, c'est-à-dire, et selon les critères désormais établis par l'autorité indépendante, dans la mise en relation automatisée d'au moins deux fichiers (en l'espèce, beaucoup plus). L'interconnexion est perçue comme un danger supplémentaire des traitements automatisés de données. La CNIL impose d'ailleurs désormais d'être informée des éventuelles interconnexions de tout fichier pour lequel elle aurait à donner un avis, ce qui est le cas (quasi-)systématiquement des fichiers de police<sup>2</sup>, c'est-à-dire des traitements automatisés de données ayant pour objectif la prévention (police administrative) ou la répression (police judiciaire) des infractions pénales.

Cette méfiance envers l'interconnexion, qu'elle soit seulement populaire, ou institutionnalisée par la loi de 1978, s'expliquerait par une plus grande atteinte aux libertés fondamentales des individus du fait même de l'interconnexion. Des fichiers interconnectés seraient plus dangereux que des fichiers isolés (en « silos »). Les raisons en sont multiples. En effet, plus les fichiers sont interconnectés, plus l'opérateur qui consulte un seul fichier interconnecté aux autres a accès à des informations diverses et complètes sur l'individu fiché. Deux problèmes au moins surgissent alors. D'une part, le principe de finalité<sup>3</sup>, qui est l'un des grands principes cardinaux du droit de la protection des données personnelles, impose que les données récoltées le soient dans un but précis et que leur usage soit ensuite conforme à cet objectif rigoureusement déterminé (pour lesquels seules les données strictement nécessaires ont été enregistrées). Or, l'interconnexion peut permettre l'accès à ces données dans un tout autre cadre, et donc dans une tout autre finalité (la CNIL dénonce d'ailleurs régulièrement l'interconnexion de fichiers relevant de finalités différentes). Les règles d'accès au fichier en sont en outre mécaniquement bousculées : chaque fichier ne doit être accessible qu'aux opérateurs qui y sont habilités et qui ont besoin d'en connaître, alors que l'interconnexion impose nécessairement des règles d'accès beaucoup plus souples et larges. Plus encore, et d'autre part, la connaissance de l'individu est beaucoup plus grande par l'interconnexion. 1+1=2 n'est pas une règle valable en matière de données personnelles, et l'interconnexion peut parfois permettre de beaucoup mieux connaître l'individu (et donc atteindre à sa vie privée), que la consultation de fichiers séparés, tant elle peut mettre en lumière des incohérences dans les discours, ou *a contrario*, mettre en évidence des rapprochements insoupçonnés entre diverses activités d'un individu (et donc accéder à une compréhension beaucoup plus fine de la personne objet du fichage). Pour ces raisons, et pour d'autres encore qu'il serait nécessaire de développer, l'interconnexion présente des dangers patents qui conduisent à une extrême méfiance en la matière.

Pourtant, les développements récents (notamment européens<sup>4</sup>, mais aussi nationaux<sup>5</sup>) des fichiers de police tendent à constater une volonté assumée des décideurs pour l'interconnexion, sans grande émotion populaire. Si cette volonté peut être justifiée par les traditionnelles nécessités de l'enquête et l'efficacité des investigations (il faudrait même « réaliser l'interconnexion des fichiers ou renoncer à toute rationalité »<sup>6</sup>, *sic!*), elle se trouve parfois défendue au nom même des libertés fondamentales. L'interconnexion permettrait une garantie plus grande des droits des individus. Les arguments se dédoublent en réalité ici. D'une part, l'interconnexion permettrait de lutter contre la fraude documentaire et la fraude aux aides sociales notamment, et servirait donc la protection des libertés fondamentales de tous les (bons?) citoyens en garantissant leur identité. L'exemple typique est ici celui des fichiers en matière de migration, donc

---

1 Le projet est notamment révélé le 21 mars 1974 par le quotidien *Le Monde*, dans un article intitulé « Safari ou la chasse aux Français » du journaliste Philippe Boucher.

2 Art. 31 à 33 de la loi *Informatique et libertés*

3 Art. 4 de la loi *Informatique et libertés*

4 Très récemment, le règlement portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration, mai 2019.

5 Le dernier grand exemple est le fichier ACCReD (décret du 3 août 2017), en matière d'enquêtes administratives.

6 Maxime CHEVALLARD, *Enjeux et perspectives des fichiers de police judiciaire : propositions pour rattraper le retard français*, Mémoire de l'École de Guerre, juin 2019

L'interconnexion serait nécessaire pour permettre de détecter les identités multiples déclarées par les migrants et donc de lutter contre l'immigration irrégulière. D'autre part, et l'argument est ici plus pernicieux encore, l'interconnexion serait un moyen de détecter plus facilement les erreurs présentes dans les fichiers de police, et de rectifier de manière plus rapide. En effet, le taux d'erreurs des fichiers de police parfois très important<sup>7</sup> serait expliqué par le fichage en « silos », qui prive la machine de la capacité de faire remonter directement aux yeux de l'opérateur les éventuelles incohérences entre les données enregistrées. Plus encore, l'interconnexion ne serait alors qu'une démarche technique, relevant de la pure administration informatique, et n'engendrerait aucune atteinte supplémentaire aux droits fondamentaux des individus. Il s'agirait simplement de garantir une meilleure fiabilité des données. Le débat démocratique est congédié, puisque la question est renvoyée à des aspects strictement techniques. Le terme même « interconnexion » disparaît souvent des propos (sans doute pour éviter de renvoyer aux souvenirs de *SAFARI*) et y est substituée la notion d'interopérabilité<sup>8</sup>, qui désigne pourtant une démarche bien moindre (puisque l'interopérabilité ne vise que la capacité de systèmes à pouvoir communiquer entre eux).

Comment expliquer cette divergence ? Comment expliquer que l'interconnexion soit passée du statut d'atteinte dangereuse aux libertés individuelles à celui d'outil bénéfique ? L'interconnexion est-elle une question de fond, qui impacte directement les libertés, et qui donc doit être débattue démocratiquement pour réaliser le meilleur équilibre entre protection des droits et garantie des libertés personnelles (ce qui est l'esprit même de la procédure pénale, et du droit des données personnelles, depuis trente ans), ou est-elle une question technique, rendue nécessaire pour fiabiliser les données ? Il s'agira de tenter de donner des éléments de réponse à ces questions, tant par des éléments strictement juridiques que par des réponses plus philosophiques et criminologiques (sur l'impact de l'interconnexion des fichiers sur le modèle libéral et démocratique notamment), et de montrer en quoi la question de l'interconnexion, qui présente pourtant un danger très grand sur les droits des individus et qui n'est pas qu'un choix technique indolore, est confisquée au débat démocratique.

---

7 La CNIL pointe ainsi régulièrement le taux d'erreur important du fichier TAJ, principal fichier policier.

8 Par exemple dans les dispositions européennes adoptées en mai 2019, cf note n°4.