Europol face aux défis posés par l'essor technologique et le traitement massif des données

par Pierre Berthelet
Docteur en droit
Chercheur associé au CESICE – Université de Grenoble-Alpes
& au CERIC – Université d'Aix-Marseille

Un constat s'impose : si Europol était confronté à un volume de données insuffisant, lié à la préférence des services répressifs et de renseignement pour la coopération bilatérale[1], la problématique tend à être désormais inverse depuis les années 2010. L'office doit traiter un volume considérable d'informations et en augmentation constate[2]. Le recours aux nouvelles technologies apparaît alors comme la solution pour traiter ce volume important de données. Celles-ci permettent non seulement d'exploiter au mieux l'information, mais aussi et surtout d'assurer sa fluidité, c'est-à-dire une meilleure circulation, non seulement entre les États membres et Europol, mais aussi entre les différents systèmes d'information de l'Union.

Dans cette optique, la problématique de la protection des données au sein du chantier de l'interopérabilité des bases de données JAI revêt une acuité toute particulière. L'innovation est au service de la gestion de l'information. Il s'agit, grâce aux nouvelles technologies, de traiter un nombre important de données et

1. M. Deflem,, « Europol and the policing of international terrorism: Counter-terrorism in a global perspective, » *Justice Quaterly*, vol. 23, n° 3, 2006, p. 353.
2. Même si l'affirmation doit être immédiatement relativisée. Cette évolution quantitative masque encore certaines difficultés d'un point de vue quantitatif puisque les États membres peinent à transférer des informations sensibles, en particulier dans le domaine de la lutte antiterroriste. Voir à ce propos le constat sévère dressé par la commission temporaire spéciale sur le terrorisme du Parlement européen (résolution du Parlement européen du 12 décembre 2018 sur les observations et les recommandations de la commission spéciale sur le terrorisme (P8_TA-PROV(2018)0512)).

ce, dans des délais toujours plus réduits. L'interopérabilité des systèmes d'information JAI s'inscrit dans cette optique : permettre à l'information de circuler afin d'avoir une vision globale des phénomènes criminels, de manière à mieux les anticiper. Or, l'interopérabilité, à l'instar des nouvelles technologies employées en matière de traitement de l'information, soulève des questions concernant le droit de la protection des données. La transparence est en effet étroitement liée à la collecte et au partage de l'information, au nom du droit à la vie privée tel que reconnu dans la Charte des droits fondamentaux[3].

Europol est donc désormais confronté au traitement d'un volume considérable d'informations (**I**). L'emploi des nouvelles technologies constitue une réponse à ce défi. Plus particulièrement, le recours à l'innovation apparaît comme une solution pour assurer efficacement la gestion de l'information (**II**). L'interopérabilité des systèmes d'information JAI constitue à cet égard, un projet visant à favoriser cette gestion. Sa mise en place pose néanmoins toute une série de questions, notamment du point de vue du respect des droits fondamentaux, en premier lieu celui de la protection des données (**III**).

I. Circulation de l'information et big data

Comme le notent Ericson et Haggerty, *« le travail de la police, beaucoup plus qu'une activité de "poursuite des criminels", est surtout un travail d'acquisition d'informations, s'appuyant sur une entreprise de production massive de données qui tend à être de plus en plus informatisée »*[4]. Ce constat est pertinent concernant Europol. Ce dernier, en réalisant des analyses criminelles, s'est positionné comme fournisseur d'expertise à l'égard des services répressifs nationaux. Or, pour produire des analyses de qualité, l'office doit être mesure de traiter un large volume d'informations. Plus ce volume est important, plus la qualité de ses productions augmente[5]. La circulation du renseignement revêt donc un caractère capital pour lui. À cet égard, le SOCTA UE, le *policy cycle* et la politique d'Europol en matière de gestion de l'information relèvent tous d'un effort commun – qui au demeurant découle d'une philosophie d'action identique, l'ILP – à savoir un meilleur partage de l'information. Ces efforts ne sont pas propres à Europol. Ils sont

3. Brouwer, E., « International cooperation and the exchange of personal data: Safeguarding trust and fundamental rights », *in* S. Carrera & V. Mitsilegas (dir.), *Constitutionalising the Security Union. Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime*, Bruxelles, Centre for European Policy Studies (CEPS), 2017, p. 78.

4. R. Ericson & K. Haggerty « La communication sur les risques, la police et le droit », *Droit et société*, vol. 47, n° 1, 2001, p. 187.

5. K. Lim, « Big data and strategic intelligence », *Intelligence and national security*, vol. 31, n° 4, 2016, p. 619-635.

consubstantiels à la coopération policière dans son ensemble, en témoignent les travaux relatifs au principe de disponibilité[6].

Comme le précise la décision 2008/615/JAI, qui constitue l'une des deux décisions destinées à transposer les dispositions du traité de Prüm consacrées à ce principe, ce dernier signifie *« tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut membre qui détient ces informations les mettant à sa disposition aux fins indiquées, en tenant compte des exigences des enquêtes en cours dans cet autre État les obtenir d'un autre État membre, les services répressifs de l'autre État »*[7]. Un tel principe fait écho au souhait émis par les chefs d'État et de gouvernement dans le programme de La Haye de novembre 2004, désireux de promouvoir une approche innovante concernant le partage transfrontalier d'informations.

Faisant le bilan de la (difficile) mise en œuvre des décisions 2008/615/JAI et 2008/616/JAI (décisions dites « Prüm ») ainsi que la décision-cadre *« suédoise »* par ailleurs, la Commission promeut, dans une communication de 2012 sur un modèle européen d'échange d'informations (EIXM), une rationalisation des canaux relatifs à l'échange d'informations[8]. Pour elle, le recours accru à Europol se justifie par ses avantages. Cette vision est, au demeurant, partagée par le Parlement européen pour qui l'optimisation de l'utilisation des instruments existants et le recours par défaut au canal d'Europol sont justifiés[9].

Une évaluation menée en 2012 révèle que les États membres n'y ont pas assez recours[10]. Cette absence de partage constitue un problème récurrent pour l'office[11]. Aux yeux du Conseil, l'accent doit être mis sur les fonctionnalités d'Europol, par exemple l'amélioration de l'application de communication sécurisée (SIENA)[12].

S'opèrent deux mouvements parallèles lors des années 2010. Le premier est le perfectionnement du *« canal Europol »* avec la création de nouvelles structures,

---

6. L. Pingel, « Le principe de disponibilité des informations dans l'espace de liberté, de sécurité et de justice », *in* Collectif, *Le droit à la mesure de l'homme. Mélanges Léger*, Paris, Pedone, 2006, p. 257-266.
7. Considérant 4 de la décision 2008/615/JAI.
8. Commission européenne, communication intitulée « Renforcer la coopération dans le domaine de la répression au sein de l'UE : le modèle européen d'échange d'informations (EIXM) » (COM(2012)735).
9. Parlement européen, résolution sur le renforcement de la coopération transfrontalière en matière répressive dans l'Union, 2013 (P7_TA(2013)0419)
10. E. Disley et *al.*, *Evaluation of the implementation of the. Europol Council Decision and of Europol's activities*, *Évaluation pour le conseil d'administration d'Europol*, Cambridge, RAND Europe / RAND Corporation, 2012.
11. O. Bures., « Europol's counter-terrorism role: A chicken-egg dilemma », *in* S. Léonard, C. Kaunert & P. Pawlak (dir.), *European homeland strategy. A European strategy in the making?*, New York, Routledge, coll. Contemporary security studies, 2012, p. 65-93.
12. Doc. du Conseil n° 9811/1/13.

par exemple, le Centre opérationnel de nouvelle génération capable de fournir un appui en temps réel à ces services (et au sein duquel figurent des analystes chargés de procéder à des recoupements ainsi qu'à des rapports analytiques), de même que le *Horizontal Operational Services* (HOS) pouvant apporter un appui en matière d'analyse stratégique aux services utilisateurs. En parallèle à ces structures sont mis en place de nouveaux instruments. C'est le cas du système d'analyse Europol (EAS) qui est un outil au service des analystes d'Europol dans le cadre des analyses stratégiques et opérationnelles menées en vertu de l'art. 4 § 1 al. f du règlement 2016/794.

Le développement des capacités d'Europol est lié à une intensification des flux d'informations inhérent à un changement d'attitude des services nationaux utilisateurs[13]. Ainsi, entre 2012 et 2013, les contributions apportées par les États membres aux fichiers de travail à des fins d'analyse ont augmenté de 40 % dans l'ensemble, à la suite de la mise en œuvre des priorités convenues dans le cadre du *policy cycle*, et de près de 60 % dans le domaine de la traite des êtres humains[14].

Cette évolution est surtout sensible après les attentats de Paris 2015[15]. Par exemple, le fichier d'analyse sur les combattants étrangers (ou *foreign fighters*) comprenait 3 600 noms de personne en 2015, et plus de 18 500 noms en 2016. De surcroît, le nombre d'unités antiterroristes ayant accès au SIENA a plus que doublé entre le début de l'année 2015 et la fin de l'année 2015. Plus de 30 unités antiterroristes y avaient en effet accès fin 2015 (et 45 fin 2016).

Ces chiffres sont confirmés par un volume important de données traitées par Europol, qu'il s'agisse du SIENA ou du Système d'information Europol (SIE). Concernant le SIENA, près d'un million de messages échangés en 2016, avec un accroissement de 19 % par rapport à 2015 (qui lui-même a enregistré un accroissement de 21 % entre 2014 et 2015). En outre, le nombre de messages antiterroristes ayant transité par le SIENA est passé de 56 000 en 2015 à près de 100 000 en 2016. Enfin, le SIENA compte 6 658 utilisateurs en 2016 (contre 5 531 utilisateurs en 2015).

Pour ce qui est du SIE, il contenait en 2016, près de 400 000 objets (soit une augmentation de 34 % par rapport à 2015) et plus de 100 000 personnes (soit une augmentation de 20 % par rapport à 2015). En outre, près d'1,5 million de recherches y ont été effectuées (soit une augmentation de 127 % par rapport à 2015). Qui plus est, le SIE devrait être mis à la disposition d'utilisateurs toujours plus nombreux au moyen du projet pilote QUEST (QUerying Europol

13. V. Amici, « Europol et la nouvelle décision du Conseil : entre opportunités et contraintes », *Revue du droit de l'Union européenne*, vol. 1, 2010, p. 93.
14. Commission européenne, communication sur le deuxième rapport sur la mise en œuvre de la stratégie de sécurité intérieure de l'Union européenne (COM(2013)179), p. 5.
15. H. Busch & M. Monroy, « Counter-terrorism and the inflation of EU databases », Statewatch, 2017. URL : https://bit.ly/2VgbIer.

SysTems). Il s'agit de permettre à ces utilisateurs de formuler une requête dans le SIE en même temps que la recherche lancée dans d'autres de données nationales et internationales. Ce projet illustre la volonté mentionnée clairement par Europol de miser davantage sur les nouvelles technologies.

II. L'innovation technologique au service de la gestion de l'information

Le recours à des technologies permet de faciliter pour l'office, l'échange d'informations, de même que la production d'une analyse de qualité. Son rapport d'activité 2016-2017 note que l'ajout de ressources analytiques supplémentaires (par exemple des analystes dont le chiffre est établi à 120 fin 2016) se heurte à un ensemble de contraintes de nature budgétaire notamment. L'emploi des technologies de l'information et de la communication (TIC) apparaît donc comme la solution[16]. Ce choix en faveur des TIC, en particulier celles les plus récentes, est clairement énoncé dans le programme de travail d'Europol de 2017 qui suggère le recours accru à l'innovation. Un tel choix se concrétise par l'élaboration d'une feuille de route consacrée aux TIC.

Quant au document de programmation du 22 janvier 2018, il promeut, dans l'*« objectif 1 »*, le développement des capacités en matière TIC en vue de maximiser l'échange d'informations. Cette orientation fait écho aux options dégagées par le règlement 2016/794 qui, lui-même, préconise que « *pour qu'Europol puisse améliorer son efficacité au niveau de la précision des analyses de la criminalité qu'elle transmet aux autorités compétentes des États membres, elle devrait recourir aux nouvelles technologies pour traiter les données. Il importe en effet qu'Europol soit en mesure de déceler rapidement les liens entre des enquêtes et les modes opératoires communs à différents groupes criminels, de vérifier les recoupements de données et d'avoir une bonne vue d'ensemble des tendances* »[17].

Les outils à disposition des services répressifs sont de plus en plus performants et le volume de données collectées et stockées est quant à lui croissant. Il s'agit donc, conformément aux principes relatifs à l'ILP, d'optimiser ce traitement afin de rendre l'information disponible. L'amélioration d'un tel traitement est un enjeu à l'heure de l'utilisation massive des nouvelles technologies et d'une recherche permanente de l'efficacité dans la lutte contre la délinquance[18]. La réponse apportée est le recours à l'innovation pour identifier les informations pertinentes.

16. D. Drewer & V. Miladinova, « The big data challenge: impact and opportunity of large quantities of information under the Europol regulation », *Computer Law and Security Review*, vol. 33, n° 3, 2017, p. 1-11.
17. Considérant 24 du règlement 2016/794.
18. N. Gerspacher, & F. Lemieux, « A market-oriented explanation of the expansion of the role of Europol: Filling the demand for criminal intelligence through entrepreneurial

Les outils mis en place par l'Internet Referral Unit (EU IRU) sont un exemple. L'EU IRU est un service de l'office chargé, conformément aux dispositions prévues de la directive 2017/541 sur la lutte antiterroriste (qui demande aux États membres d'agit rapidement pour supprimer les contenus en ligne incitant à commettre des actes terroristes), d'opérer une surveillance d'Internet en vue de la suppression de contenus illicites, en premier lieu ceux relatifs à la propagande djihadiste. Cette surveillance s'opère en liaison avec les services répressifs nationaux et le secteur privé : les premiers signalent à Europol un contenu pour évaluation, les seconds sont destinataires, une fois cette dernière réalisée, d'une demande de suppression[19]. Dans cette perspective, l'EU-IRU dispose d'outils technologiques performants, à la fois pour réaliser une surveillance effective du web, et pour assurer rapidement une évaluation de même qu'un suivi des demandes de suppression[20].

Cette inclinaison d'Europol en faveur des technologies innovantes fait également écho aux conclusions du Conseil des 4 et 5 décembre 2014 instituant une stratégie actualisée sur la gestion de l'information pour la sécurité intérieure de l'Union[21]. Une telle stratégie, qui remplace celle de 2009, part du constat que le volume des échanges transfrontières d'informations s'est considérablement accru ces dernières années et qu'à ce titre, le recours à la technologie, en particulier l'automatisation, est un moyen d'assurer une gestion efficace du flux de données. Or, d'après le texte, cet échange transfrontière constitue une condition préalable pour atteindre les objectifs de sécurité intérieure dans l'Union. Une telle stratégie entend donc faciliter la circulation de l'information entre les États membres.

Faisant écho aux prescriptions du programme de Stockholm pour qui le développement de la gestion et des échanges d'informations doit se réaliser de façon cohérente et structurée, il s'agit d'encourager les travaux sur les modalités technologiques du partage d'informations (notamment concernant le format universel pour les messages (UMF), comme norme commune en vue de favoriser les interactions entre les divers systèmes, de manière à assurer un échange structuré) et de favoriser l'interopérabilité en vue d'améliorer la synergie des systèmes d'information.

À cet égard, l'interopérabilité est devenue, depuis la stratégie de 2014 sur la gestion de l'information pour la sécurité intérieure de l'UE, l'un des principaux chantiers de la coopération policière. Déjà évoquée au milieu des années 2000[22],

---

initiatives », *in* Lemieux, F. (dir.), *International police cooperation. Emerging issues, theory and practice*, Cullompton, Willan Publishing, 2010, p. 68.

19. p. 16 du doc. du Conseil n° 9646/17.

20. J. Ellermann, « Terror won't kill the privacy star – tackling terrorism propaganda online in a data protection compliant manner », ERA Forum, n° 17, 2016, p. 4.

21. Doc. du Conseil n° 15701/1/14.

22. V. Mitsilegas, « Police co-operation: What are the main obstacles to police co-operation in the EU? », *in* A. Baldaccini et *al.* (dir.), *Controlling security*, Centre d'Études sur les Conflits, coll. Cultures et conflits, Paris, L'Harmattan 2008 p. 11-12.

elle est liée à la multiplication des bases de données JAI et à la volonté des services de police des États membres d'y être connectés[23]. Elle découle du fait que face à des menaces évolutives, l'interopérabilité des bases de données (comme prolongement d'une plus grande circulation d'informations destinée à éviter toute surprise stratégique) est une solution privilégiée[24]. Elle vise à assurer une fluidité dans le partage d'une information numérisée et stockée dans des bases de données sécuritaires, qu'elles soient ou non gérées par Europol.

Contrairement au principe de disponibilité, elle requiert, non seulement la disponibilité des informations, mais aussi l'interconnexion, à des degrés divers, des systèmes d'information existants[25]. En effet, elle relève de l'idée que l'information est déjà présente, mais le compartimentage des systèmes empêche sa circulation.

III. L'interopérabilité des systèmes d'information, un problème de protection des données

La Commission a présenté, le 6 avril 2016, une communication qui part du constat identique à celui formulé dans la stratégie de 2014, à savoir une fragmentation de l'échange d'informations. Notant à ce propos qu'il *« existe un certain nombre de systèmes d'information à l'échelle de l'Union qui fournissent aux garde-frontières et aux policiers des informations utiles sur les personnes, mais l'architecture européenne de la gestion des données n'est pas parfaite »*, il s'agit dès lors d'*« optimiser les avantages des systèmes d'information existants [et de] concevoir, si nécessaire, de nouvelles actions complémentaires visant à combler les lacunes »*[26]. Cette communication a débouché sur la présentation de deux propositions de règlement. Présentés le même jour, ces règlements visent à définir les quatre *« composantes techniques »* destinées à concrétiser ce projet d'interopérabilité, appelé de ses vœux par la Stratégie de sécurité intérieure 2015-2020.

Entrent dans le champ de ces règlements, six systèmes d'information de l'Union ainsi que deux systèmes Interpol. A priori, le projet ne concerne Europol qu'à la marge. En effet, les bases de données de l'office ne sont pas incluses dans ce

23. G. de Kerchove, « Brèves réflexions sur la coopération policière au sein de l'Union européenne », *Revue de sciences criminelles et de droit pénal comparé*, n° 3, 2004, p. 553-569.
24. M. den Boer, « Counter-terorism, security and intelligence in the EU : governance challenges for collection, exchange and analysis », *Intelligence and national security*, vol. 30, n° 2-3, p. 407.
25. D. Curtin, « Security of the interstice and interoperable data sharing: A first cut in Constitutionalising the Security Union », *in* S. Carrera & V. Mitsilegas (dir.), *op. cit.,* p. 65-72.
26. Commission européenne, communication intitulée « Des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité » (COM(2016)205), p. 2.

chantier destiné à mettre fin à la mosaïque existante de systèmes JAI. Les données d'Europol sont englobées dans le dispositif des règlements uniquement dans la mesure où cela est pertinent pour le fonctionnement de l'un des six systèmes évoqués (en l'occurrence ETIAS).

Toutefois, l'implication d'Europol est moins périphérique qu'il n'y paraît. D'abord, les projets technologiques, tels que QUEST, font écho à l'une des composantes techniques, à savoir la création d'un portail européen de recherche (ESP) (déjà mentionné par la communication de la Commission de 2012 sur l'EIXM). Ensuite, Europol est évoqué par ces propositions de règlement, au même titre qu'Interpol, pour favoriser le recours à la norme UMF dans le développement de ses systèmes. Surtout, l'office est inclus, aux côtés d'autres agences (EU-LISA), dans la structure de gouvernance pilotée par la Commission, et destinée à assurer le déploiement de l'UMF.

Enfin, il a pris part, aux côtés d'autres agences, comme EU-LISA et l'Agence européenne de garde-frontières, au groupe d'experts créé par la Commission suite de sa communication d'avril 2016. Autrement dit, l'office a largement contribué aux recommandations figurant dans le rapport final publié en mai 2017 et rédigé par ce groupe d'experts, réuni pour la première fois en juin2016. Or, les recommandations préconisées par ce rapport, validées par le Conseil en juin 2017[27], ont constitué le point de départ de la préparation, par la Commission, de ses propositions de règlement sur l'interopérabilité.

La Commission précise bien dans ses propositions, que ces composantes techniques ne modifient pas l'architecture des systèmes existants. En effet, les solutions d'interopérabilité proposées ne constituent *« que des éléments complémentaires des systèmes existants. En tant que telles, elles ne modifieront pas l'équilibre déjà garanti par chacun des systèmes centraux existants en ce qui concerne leur incidence positive sur les droits fondamentaux »*[28]. Les atteintes éventuelles aux droit fondamentaux respectent, selon le principe de proportionnalité tel que mentionné par la Charte (art. 52 § 1).

Pourtant, cette affirmation est de nature à prêter le flanc aux critiques au motif que ces modifications anodines entraînent, au final, des atteintes sensibles à la protection des données[29]. Le danger n'est alors pas le projet relatif à l'interopérabilité en tant que tel. Il s'agit de l'accumulation des projets sécuritaires, c'est-à-dire l'environnement sécuritaire dans lequel s'insère l'interopérabilité faisant que leur combinaison constitue le caractère intrusif à la vie privée. Les conclusions du Conseil sur l'EIXM avaient indiqué que *« la préservation des droits fondamentaux, en particulier le droit à la vie privée et à la protection des données,*

27. Doc. du Conseil n° 9448/17.
28. T. Bunyan, « The interoperability of Justice and Home Affairs databases », Statewatch, Briefing, 2018, p. 2. URL : https://bit.ly/2XvSQ8P.
29. Commission européenne, 2017, proposition de règlement consacré à l'interopérabilité (COM(2017)793), p. 29.

devrait être un principe cardinal de l'échange d'informations en matière répressive »[30]. Cet impératif avait déjà été répété par le Contrôleur européen à la protection des données (CEPD) pour qui l'application de l'interopérabilité des systèmes d'information doit se réaliser en parfait accord avec les différents principes de la protection des données, en particulier celui de la finalité, tel que désormais mentionné désormais dans la directive (UE) 2016/680 sur la protection des données en matière pénale (art. 4 § 1 al b).

Quant à l'Agence européenne des droits fondamentaux, elle s'inquiète de ce projet, notamment au motif qu'elle est de nature à établir un mécanisme de profilage racial, contraire aux dispositions de la directive 2000/43 qui précisément, promeut un traitement égalitaire[31]. Plus généralement, l'enjeu actuel de l'interopérabilité est résumé par le professeur Deirdre Curtin de la manière suivante : *« le domaine de la sécurité et de la police est celui où la collecte d'informations, le* data mining *et le partage d'informations entre systèmes interconnectés sont très largement invisibles, mais en même temps soumis à une coopération accélérée et intensifiée. Il est fait usage de vastes réseaux d'"euro-cops" pour [permettre à Europol] de faire son travail de manière "efficace". Le problème est, comment rendons-nous l'invisible transparent ? Et comment pouvons-nous rendre des arrangements informels, invisibles et multi-juridictionnels responsables* (accountable) *? »*.

En conclusion, la question de la transparence numérique, largement discutée au sujet des algorithmes, concerne également Europol. L'office fait de la question de la gestion de l'information par le développement d'outils innovants en matière de traitement des données, une thématique centrale de son développement. Se pose alors le problème de la transparence de son activité au moment où les enjeux de la protection des données se déplacent sur le terrain de l'interopérabilité des systèmes d'information de l'Union.

30. Doc. du Conseil n° 9811/1/13, p. 3.
31. European Union Agency for Fundamental Rights (EUAFR), *Fundamental rights and the interoperability of EU information systems : borders and security*, Vienne, 2017, p. 43.