Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe

Intervention au colloque sur l'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne (CESICE, Université Grenoble-Alpes, 18 novembre 2016)

par Bertrand WARUSFEL,
Professeur à l'Université de Lille 2 (CRDP), avocat au barreau de Paris

La culture du secret, en tant que pratique sociale des institutions de police et – plus encore – de renseignement a précédé historiquement l'organisation juridique des secrets de l'État. Mais inversement, l'existence dans tous les pays de l'Union d'une législation protégeant les secrets nationaux est aujourd'hui cause ou prétexte des réticences à développer l'échange multilatéral de données de sécurité au sein de l''espace européen de liberté, de sécurité et de justice.

Les obligations légales de protection des secrets nationaux

Partant du cas (assez représentatif, au moins au niveau des principes) du droit français du secret de la défense nationale, on peut dégager plusieurs caractéristiques prégnantes de ces systèmes nationaux de protection du secret :

- leur protection repose sur la combinaison d'un mécanisme de classification des informations à protéger (en plusieurs catégories en fonction de leur sensibilité croissante), d'une exigence d'habilitation préalable des personnes pouvant y accéder, ainsi que de la règle du « besoin d'en connaître » (qui ne permet à une personne d'accéder qu'aux secrets qui sont directement utiles à sa mission, à l'exception des autres, même de niveau équivalent). La violation de ces obligations est sanctionné pénalement et peut constituer un crime de trahison ou d'espionnage lorsqu'elle est commise au bénéfice de l'étranger et qu'elle pourrait causer un préjudice à ce que le code pénal français dénomme « les intérêts fondamentaux de la nation ».

- Ces secrets nationaux (secret de la défense nationale en France, « official secrets » en Grande-Bretagne, …) ne couvrent pas seulement des informations relatives à la sécurité militaire ou extérieure de l'État, mais plus largement toutes informations dont la connaissance pourrait nuire gravement à la sécurité de la collectivité, c'est-à-dire à la « sécurité nationale » au sens que lui donne désormais l'article L.1111-1 du code de la défense français. En particulier, des informations relevant de la police administrative ou du renseignement criminel sont fréquemment classifiées. Ces classifications nationales s'appliquent donc à de nombreuses données susceptibles d'être échangées au sein de l'espace européen de liberté, de sécurité et de justice.

- Mais par ailleurs ces classifications nationales (ou transnationales, comme le secret OTAN ou UE) ne sont généralement pas susceptibles d'être communiquées et partagées dans le cadre de procédures judiciaires. Le secret de défense français est resté impénétrable aux juridictions (administratives, civiles ou pénales). Il en va plus ou moins de même dans les autres États, même si plusieurs connaissent des mécanismes de conciliation plus ou moins limités (comme le

recours à des « special advocates » au Royaume-Uni). En France, on a créé en 1997 une commission consultative (CCSDN) servant d'intermédiaire entre les secrets de l'exécutif et la justice. Et tout récemment, la nouvelle loi sur le renseignement du 24 juillet 2015 a créé un recours spécial devant le Conseil d'État, auquel (pour la première fois) les services de renseignement ne peuvent plus opposer le secret (mais cela reste limité au seul cas du contrôle de la légalité des techniques de renseignement).

Des pratiques de cloisonnement et de diffusion contrôlées des informations qui limitent le partage multilatéral des données de sécurité

Il faut noter, tout d'abord, que pour un service qui recueille de l'information par le biais de sources humaines ou techniques clandestines, la classification se justifie non seulement par la sensibilité intrinsèque du renseignement recueilli, mais aussi – voire surtout – par ce qu'il pourrait révéler de la source dont il est issu et des méthodes qui ont été mise en œuvre pour son recueil. Cet objectif de « protection des sources et des méthodes » est un principe quasi-sacré pour un service de renseignement et justifie en pratique un recours abondant à la classification d'informations qui, en eux-mêmes, pourraient sembler peu compromettants voire qui sont parfois rendus publics par ailleurs.

Pour rendre malgré tout possible la circulation transfrontalières d'informations classifiées, en particulier entre États alliés (ou membres de l'Union européenne), la pratique est de conclure des accords de sécurité bilatéraux (ou parfois multilatéraux comme en ce qui concerne les secrets de l'OTAN ou de l'Union européenne). Ces accords établissent une équivalence entre les niveaux de classification des différentes parties et leur imposent chacune de protéger chez elle les secrets des autres comme les siennes. Il instaure une forme de reconnaissance mutuelle des secrets et des habilitations de sécurité et permet une circulation contrôlée des données classifiées d'un État à l'autre.

Mais ces accords comportent tous des clauses interdisant à l'État receveur de rediffuser ou de partager à nouveau les données classifiées reçues sans l'accord de l'État d'origine. Cela est conforme à une autre règle cardinale de la pratique des services de renseignement, celle dite du « tiers service » (« originator control » en anglais). En pratique, c'est le service émetteur qui garde ce que l'on a coutume d'appeler la « propriété du renseignement » que le service receveur ne peut enfreindre, faute de rompre la confiance et de bloquer la coopération.

Ce principe du tiers service il limite, en pratique, largement la facilitation de circulation des données que rendent possible les accords de sécurité. En particulier, il incite fortement les services à privilégier les échanges bilatéraux (basé sur le donnant-donnant et le contrôle réciproque des renseignements échangés) sur le partage en multilatéral, qui paraît rendre plus difficile la traçabilité et la maîtrise des données secrètes. Par ailleurs, il incite aussi les services à préférer partager des synthèses plutôt que des renseignements bruts, dont la dissémination pourrait plus facilement porter atteinte au secret des sources et méthodes.

Cela constitue enfin souvent un obstacle à l'exercice par les institutions nationales compétentes d'un contrôle indépendant (que la garantie des droits fondamentaux, telle

qu'interprétée par la CEDH, impose de mettre en œuvre pour encadrer les pratiques clandestines des États justifiés par les impératifs de sécurité). Dans beaucoup d'États, en effet, une part importante des renseignements collectés et exploités proviennent des échanges avec les services tiers, ce qui bloque largement l'efficacité du contrôle.

Conclusion

Toutes ces contraintes freinent encore les avancées vers une plus grande intégration du renseignement de sécurité au niveau de l'Union européenne.

Mais si le développement d'agences européennes intégrées paraît une approche inappropriée, on doit espérer en revanche que les circuits de coopération et d'échange de données vont se renforcer sans pour autant démanteler les dispositifs nationaux de protection du secret, dont l'importance est réelle pour mener la lutte contre les menaces les plus dangereuses contre nos collectivités (terrorisme, ingérences étrangères, cybercriminalité, organisations criminelles transnationales, …) mais plutôt à en contournant les effets potentiellement bloquants.

C'est ainsi qu'Europol dispose déjà de règles de confidentialité lui permettant de discuter avec les États-membres de l'opportunité de maintenir des niveaux de secret qui paraîtraient inadaptés.

Mais c'est surtout en aval, au niveau du contrôle par les institutions indépendantes qu'il faut imaginer que ces organes essentiels de l'État de droit puissent coopérer entre eux pour faire advenir un standard européen des pratiques de renseignement et de protection du secret et permettre une entraide efficace, par exemple en permettant à l'autorité de contrôle du service récepteur de saisir celle de l'État du service émetteur afin qu'elle effectue pour son compte certaines vérifications, tout en respectant la souveraineté nationale de chacun.

Ce droit européen du renseignement favoriserait ensuite par ricochet la possibilité de développer des instruments multilatéraux réellement efficaces entre les États-membres. Et il trouverait assez logiquement sa place à côté du droit européen des libertés fondamentales et de celui de la protection des données personnelles.

B. Warusfel