Conseil de
l'Union européenne

Bruxelles, le 23 novembre 2015
(OR. en)

14369/15

JAI 895
COPEN 319
DROIPEN 150
CYBER 110

NOTE

Origine:	la présidence
Destinataire:	Comité des représentants permanents/Conseil
Nº doc. préc.:	13689/15
Objet:	Une justice pénale efficace à l'ère du numérique - quels sont les besoins - État d'avancement des travaux

1. Le rapport sur l'évaluation de la menace que représente la criminalité organisée sur l'internet en 2015 (iOCTA)[1] conclut que la cybercriminalité est de plus en plus agressive et source de conflits et englobe un éventail extrêmement varié d'activités criminelles, y compris des infractions traditionnelles qui laissent des traces numériques. Cette approche qui consiste à exercer des pressions sur les personnes et les entreprises est révélatrice de l'évolution du profil des cyberdélinquants et peut laisser penser que leurs activités relèvent aussi de la criminalité organisée tout en mettant en lumière l'impact psychologique croissant de la cybercriminalité sur les personnes qui en sont victimes.

2. Les nouvelles évolutions et innovations technologiques représentent des défis spécifiques pour la conduite d'enquêtes efficaces et accroissent la pression exercée sur les systèmes de justice pénale pour qu'ils adaptent leurs outils et leurs méthodes en conséquence, ce qui revêt une importance particulière dans le contexte des politiques de lutte contre le terrorisme et des mesures de lutte contre la radicalisation: Les canaux de communication internet et les multiples médias sociaux, y compris les techniques de cryptage, constituent autant de modes opératoires largement utilisés à des fins terroristes.

[1] doc. 12728/15

3. Dans un environnement technologique en évolution si rapide, les données électroniques revêtent une importance croissante dans le cadre des procédures pénales. Ces données constituent des preuves électroniques. Toutefois, les difficultés rencontrées pour recueillir et produire en justice des preuves électroniques recevables et obtenir une condamnation définitive des contrevenants persistent. Cet état de fait incite à évaluer les outils juridiques et pratiques dont disposent actuellement les autorités compétentes à l'aune des besoins d'une justice pénale efficace à l'ère du numérique.

4. Dans le prolongement des discussions menées au sein du CATS le 10 novembre 2015, le présent document expose en annexe un certain nombre d'axes de travail que les ministres de la justice devraient examiner en vue de fournir des orientations sur la voie à suivre pour relever les défis liés à la collecte et à l'utilisation des preuves électroniques dans les procédures pénales.

Les ministres sont invités à indiquer parmi les questions exposées dans le présent document lesquelles devraient être traitées en priorité.

Ces questions peuvent être résumées comme suit:

- Les difficultés posées par les processus de perte de données dans un environnement numérique qui peuvent nuire à l'efficacité des enquêtes pénales, y compris l'incidence qu'un régime efficace de conservation des données peut avoir à cet égard.

- Les problèmes auxquels les autorités compétentes sont confrontées lors de l'application des règles traditionnelles d'entraide judiciaire, en particulier en ce qui concerne les exigences formelles requises pour traiter une demande d'entraide judiciaire ou la rapidité de la procédure ainsi que l'effet qu'une utilisation optimale de la décision d'enquête européenne pourrait avoir sur les affaires relevant de l'UE.

- La nécessité d'optimiser le cadre de coopération avec les prestataires de services étrangers lorsque la pratique existante des autorités compétentes consistant à leur adresser directement des demandes doit être réexaminée à la lumière des préoccupations grandissantes en matière de droits fondamentaux et de garanties procédurales.

- Les conséquences juridiques liées à la localisation et à la propriété d'importantes infrastructures numériques, et en particulier le renforcement du dialogue avec les autorités américaines à cet égard.

- Les difficultés spécifiques posées par l'informatique en nuage, souvent désignées comme "perte de localisation", et les incidences qu'elles ont sur les règles de compétence applicables, ainsi que la possibilité d'envisager un accès transfrontalier aux données pour faire face aux situations où la localisation des données n'est pas connue.

- La complexité découlant de la diversité des règles et normes en matière de recevabilité des preuves électroniques devant les juridictions nationales compétentes.

- La nécessité d'évaluer toute mesure ou initiative améliorant l'efficacité des procédures pénales à l'ère du numérique à l'aune des exigences de la Charte des droits fondamentaux de l'UE et des normes de la CEDH dans l'interprétation qu'en donne la Cour européenne des droits de l'homme.

ANNEXE

Difficultés liées à la collecte et à l'utilisation de preuves électroniques dans les procédures pénales

1. La collecte efficace, la transmission et la recevabilité des preuves électroniques[2] dans les procédures pénales présentent d'importantes difficultés du point de vue de la justice pénale. C'est ce qu'ont confirmé les premiers rapports par pays publiés dans le cadre de la *septième série d'évaluations mutuelles consacrées à la mise en œuvre pratique et au fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre ce phénomène* et diverses discussions menées sur des questions liées aux preuves électroniques, notamment lors de la réunion informelle COSI-CATS des 22 et 23 juillet 2015 et d'un atelier sur l'entraide judiciaire à l'ère du numérique organisé le 15 octobre 2015 par la présidence avec l'Université de Luxembourg.

2. Le 19 octobre et le 11 novembre 2015, le groupe des Amis de la présidence chargé des questions inhérentes au cyberespace a examiné, comme le prévoyait la liste d'actions prioritaires en vue de la mise en œuvre de la stratégie de sécurité intérieure renouvelée pour l'Union européenne, les failles (juridiques) de la lutte contre la cybercriminalité afin de rechercher des approches globales visant à lever les obstacles aux enquêtes sur la cybercriminalité ainsi qu'à apporter à la Commission une contribution pratique concernant d'éventuels nouveaux instruments législatifs, de mieux sensibiliser et de partager les bonnes pratiques[3].

3. Dans le prolongement de ces discussions, le présent document se fonde sur la contribution qu'Eurojust a apportée sur la base des dossiers qu'il traite, des rapports finals du séminaire sur la cybercriminalité qu'il a organisé les 19 et 20 novembre 2014 et de la réunion tactique qu'il a consacrée à la cybercriminalité le 1er juillet 2015. Parmi les autres sources utilisées pour élaborer le présent document figurent un certain nombre de rapports ciblés du comité de la convention du Conseil de l'Europe sur la cybercriminalité[4], l'iOCTA élaboré par Europol/EC3, les résultats de l'atelier susmentionné de la présidence sur l'entraide judiciaire à l'ère du numérique ainsi que la récente étude commandée par la commission LIBE du Parlement européen sur les défis que pose la cybercriminalité en matière de répression[5]. Il tient également compte des observations formulées par les États membres lors de la réunion du CATS du 10 novembre 2015.

---

2 Aux fins du présent document, l'expression "preuves électroniques" renvoie à toutes les données électroniques relatives à une infraction pénale, qui peuvent être utiles dans le cadre de procédures pénales. La collecte, le partage et l'utilisation de données aux seules fins de désorganisation ou de prévention ne sont donc pas traitées dans ce document.

3 doc. 12612/15

4 http://www.coe.int/en/web/cybercrime/t-cy-reports

5 EP LIBE Committee(2015), Study "The law enforcement challenges of cybercrime: are we really playing catch-up?" (Les défis en matière de répression de la cybercriminalité: sommes-nous réellement en phase de rattrapage?), PE 536.471

1. Conservation des données et perte de données

4. La directive 2002/58/CE (la directive "vie privée et communications électroniques) énonce des règles spécifiques concernant le traitement des données à caractère personnel dans le secteur des communications électroniques tout en prévoyant le droit à la confidentialité des communications (article 5) et l'obligation pour les fournisseurs de services d'effacer les données relatives au trafic lorsqu'elles ne sont plus nécessaires aux fins de la transmission d'une communication, à moins qu'elles ne soient traitées dans certaines conditions aux fins de la facturation des abonnés et des paiements pour interconnexion. L'article 15, paragraphe 1,[6] autorise dans certaines conditions à limiter les droits et obligations prévus par la directive pour un ensemble de finalités spécifiques, et notamment pour "*assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales".* À cet égard, la mise en place dans certaines conditions de mesures nationales de conservation des données est autorisée. La directive 2006/24/CE (la directive sur la conservation des données) visait à harmoniser ces règles en vue de garantir la disponibilité des données à des fins de recherche, de détection et de poursuite d'infractions graves.

5. De par leur nature, la durée de vie des preuves électroniques est courte. En outre, l'essor que connaît l'usage privé de la diffusion en direct, le cryptage, le développement du Darknet et l'anonymisation permettent aux criminels de dissimuler complètement des preuves déterminantes aux services répressifs. Ainsi, des preuves électroniques déterminantes peuvent être perdues si les autorités compétentes ne disposent pas de moyens adéquats pour réagir efficacement. L'existence d'un système efficace de conservation des données pourrait se révéler très utile à cet égard.

---

[6] L'article 15, paragraphe 1, de la directive 2002/58/CE est libellé comme suit:
"Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne."

6. Eurojust explique dans son analyse du cadre juridique des États membres de l'UE et des défis actuels en matière de conservation des données en date du 26 octobre 2015[7] que l'actuelle fragmentation du cadre juridique en matière de conservation des données dans l'ensemble de l'UE à la suite de l'invalidation de la directive 2006/24/CE (la directive sur la conservation des données) par l'arrêt de la Cour de justice de l'Union européenne du 8 avril 2014 a une incidence sur l'efficacité des enquêtes et des poursuites pénales au niveau national, en particulier en termes de fiabilité et de recevabilité des preuves en justice, ainsi que sur la coopération judiciaire transfrontalière entre États membres et au niveau mondial.

7. Les ministres procèderont à un examen spécifique de l'état actuel de la situation et des effets de l'arrêt sur la conservation des données rendu par la Cour le 8 avril 2014, examen auquel sera consacré un point distinct de l'ordre du jour du Conseil.

2. Processus d'entraide judiciaire

8. La collecte de preuves électroniques est en principe une question pour laquelle le facteur temps est essentiel. L'existence de procédures rapides pour la conservation et la collecte des données électroniques est cruciale pour assurer le déroulement efficace des procédures pénales. Étant donné que les données électroniques sont très souvent localisées sur un territoire étranger, les autorités compétentes nationales doivent utiliser les outils de coopération internationale existants, c'est-à-dire les demandes d'entraide judiciaire ou, si la procédure concerne les États membres de l'UE, recourir, le cas échéant, aux instruments de reconnaissance mutuelle existants dans le domaine de la coopération judiciaire en matière pénale.

9. La directive 2014/41/UE concernant la décision d'enquête européenne[8] revêt une importance particulière à cet égard. À compter du 22 mai 2017, elle remplacera la législation fragmentée de l'UE existante relative à la collecte et au transfert des éléments de preuve entre États membres de l'UE avec pour objectif de rendre les enquêtes transfrontières plus rapides et plus efficaces. Il devrait être fait pleinement usage de ce système dans le cadre du champ d'application de la décision d'enquête européenne également en ce qui concerne les preuves électroniques.

---

[7] doc. 13085/15

[8] JO L 130 du 1.5.2014, p. 1.

10. Souvent, les données électroniques se trouvent à l'étranger sur le territoire d'États tiers. Dans de tels cas, il convient de procéder à une demande d'entraide judiciaire. Les régimes existants en matière d'entraide judiciaire sont toutefois toujours davantage perçus comme étant trop lents et pesants pour faire face aux contraintes de temps. Ainsi, la question se pose de savoir ce qui pourrait être fait pour accélérer le processus d'entraide judiciaire, en premier lieu pour optimiser les procédures existantes. À cet égard, il serait possible d'envisager l'élaboration d'un formulaire de demande standardisé, simplifié et qui pourrait éventuellement être transmis et accepté en ligne, notamment dans le cadre de la décision d'enquête européenne. On pourrait également examiner si les exigences formelles prévues dans les procédures d'entraide judiciaire pourraient être davantage différenciées en fonction du type de données demandées - s'agit-il, par exemple, de données concernant un abonné, le trafic ou le contenu. Dans de nombreuses juridictions, les conditions d'accès aux données relatives aux abonnés sont généralement moins strictes que pour l'accès aux données relatives au trafic, tandis que le régime le plus strit s'applique aux données relatives au contenu[9].

11. Il serait possible d'établir une norme commune permettant de traiter une demande de coopération comme "urgente". En outre, il serait possible d'envisager des procédures rapides de transfert des éléments de preuve dans certaines conditions comme il en existe pour la conservation des éléments de preuve en application des dispositions pertinentes de la convention du Conseil de l'Europe sur la cybercriminalité. En règle générale, dans la situation actuelle, même si les preuves sont conservées, il faut parfois beaucoup de temps pour qu'elles soient disponibles aux fins de la procédure pénale dans le pays demandeur.

12. Pour rendre opérationnel le processus de coopération, il devrait être envisagé d'assurer une coordination préalable et d'associer les autorités judiciaires à la procédure pénale à un stade précoce. À cet égard, il pourrait être envisagé de renforcer encore les réseaux de coopération joignables 24 h sur 24, y compris ceux des autorités judicaires, et notamment de mettre en place un réseau de procureurs traitant des affaires relatives à la cybercriminalité. Cela contribuera à favoriser et renforcer les contacts directs entre autorités judiciaire, y compris en ce qui concerne les demandes d'entraide judiciaire dans l'ensemble de l'UE et au niveau mondial. À cet égard, il convient d'examiner le rôle d'Eurojust et d'Europol/EC3.

---

[9] Voir le document de réflexion du T-CY "Défis de l'accès de la justice pénale aux données stockées dans le nuage", mai 2015 (T-CY(2015)10), p. 7 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

3. Demandes directes et coopération avec les prestataires de services étrangers

13. Une coopération avec le secteur privé est indispensable pour lutter contre la cybercriminalité. Il n'existe cependant pas de cadre juridique commun applicable à ce type de coopération. Or, cette question revêt une importance particulière lorsqu'il s'agit d'obtenir l'accès à des données détenues par des prestataires de services étrangers.

14. Pour surmonter les inconvénients de la procédure d'entraide judiciaire actuelle en ce qui concerne la collecte de preuves électroniques, les autorités compétentes peuvent recourir à d'autres méthodes d'obtention de preuves numériques, par exemple en adressant directement une demande aux prestataires de services étrangers. En pareils cas, il se peut que les prestataires de services soient autorisés en vertu de la législation de leur pays à divulguer à des services répressifs (étrangers), sur une base volontaire, des données ne se rapportant pas au contenu. Toutefois, ce n'est pas le cas dans tous les États. Par ailleurs, les prestataires de services ne sont pas toujours disposés à coopérer, même si la législation nationale le permet. De même, tous les États membres n'autorisent pas qu'une injonction interne de production de données soit adressée à une entité privée située à l'étranger. Il est aussi possible qu'une preuve électronique, même si elle a été obtenue par divulgation volontaire, ne soit pas recevable devant la juridiction de l'État requérant car elle a été obtenue en dehors du cadre de l'entraide judiciaire. D'une manière générale, ainsi qu'il a été relevé lors de l'atelier organisé le 15 octobre par la présidence sur l'entraide judiciaire à l'ère du numérique, un tel mécanisme pourrait donner lieu à un phénomène susceptible d'être défini comme une entraide judiciaire sans véritable entraide, ce qui pourrait susciter des inquiétudes quant aux droits fondamentaux et aux garanties procédurales.

15. Du fait que l'on s'adresse directement à eux, les prestataires de services étrangers pourraient par ailleurs se trouver confrontés à des demandes contradictoires émanant de différents États mais aussi être soumis à des exigences contradictoires en termes de protection de la vie privée et de garanties procédurales s'ils exercent leurs activités dans plusieurs pays. Par exemple, des prestataires de services pourraient enfreindre les règles d'un État en matière de protection des données s'ils divulguent des données aux autorités d'un autre État.

16. Compte tenu de tout ce qui précède, il est indispensable de fixer des conditions claires pour un cadre de coopération durable entre acteurs privés et pouvoirs publics aux fins de la collecte de preuves électroniques, reposant, d'une part, sur le respect absolu des garanties procédurales accordées aux suspects et aux personnes poursuivies dans le cadre de procédures pénales et, d'autre part, sur la protection des données à caractère personnel.

4. Conséquences juridiques liées à la localisation et à la propriété d'une infrastructure numérique

17. Compte tenu des effets que la législation de l'État d'exécution pourrait avoir sur le processus de coopération internationale, il est essentiel de renforcer le dialogue avec les pays qui sont des acteurs clés s'agissant du fonctionnement et de la propriété des grandes infrastructures numériques.

18. Cette question est particulièrement importante dans le cas de la coopération avec les États-Unis. Dans son étude de 2015 sur les défis en matière de répression de la cybercriminalité, la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) a déclaré que des entreprises américaines et des entreprises installées aux États-Unis jouaient un rôle de premier plan dans le fonctionnement de l'Internet. En conséquence, le cadre juridique américain a une incidence considérable sur la répression de la cybercriminalité[10]. Au-delà de la question des différences de normes en matière de protection des données, du point de vue de la justice pénale au sens strict, cette situation a des répercussions sur la norme qu'il convient de respecter pour justifier juridiquement les demandes d'entraide judiciaire adressées aux États-Unis, en particulier lorsque les demandes portent sur des données relatives au contenu.

19. En règle générale, toutes les demandes d'entraide judiciaire doivent comporter une explication des raisons pour lesquelles l'autorité compétente a un intérêt légitime à obtenir les données demandées. La législation américaine exige que les demandes soient appréciées au regard de la norme dite de la "cause probable", qui est une norme de justification plus élevée par rapport à la notion de "suspicion raisonnable" ou son équivalent. La justification reposant sur la "cause probable" limite les interventions des autorités compétentes à ce qui est strictement nécessaire aux fins de l'enquête spécifique. C'est pourquoi il est très probable qu'une demande d'entraide judiciaire soit rejetée par les autorités américaines parce qu'elle ne satisfait pas à l'obligation de justifier une "cause probable". Il convient aussi d'assurer un juste équilibre entre les possibilités qu'ont les autorités américaines et étrangères de recevoir un accès à des données américaines "locales", d'une part, et à tout autre type de données, d'autre part. Ces questions devraient être abordées via un dialogue permanent entre l'UE et les États-Unis, notamment dans le cadre du processus de réexamen de l'accord sur l'entraide judiciaire avec l'UE.

---

10 Étude (2015) de la commission LIBE du Parlement européen "The law enforcement challenges of cybercrime: are we really playing catch-up?" (Les défis en matière de répression de la cybercriminalité: sommes-nous réellement en phase de rattrapage?), PE 536.471, p. 46.

5. Disparition du lieu

20. Si l'accès à des preuves électroniques dans des ressorts territoriaux étrangers intervient essentiellement dans le cadre de l'entraide judiciaire, le recours croissant à l'informatique en nuage et aux services fondés sur le web constitue un défi supplémentaire pour les autorités compétentes, décrit comme une "disparition du lieu"[11]. Dans ce cas, la preuve électronique est stockée "quelque part dans le nuage", soit sur un seul serveur soit répartie sur plusieurs serveurs, voire déplacée entre serveurs à différents endroits. Ainsi, les données concernées sont situées physiquement dans un ressort territorial étranger ou inconnu, ou encore dans plusieurs ressorts territoriaux en même temps ou se déplacent entre différents ressorts territoriaux.

21. En principe, le lieu détermine les autorités compétentes et la législation applicable à l'enquête, y compris la mesure dans laquelle des pouvoirs coercitifs pourraient être exercés, ainsi que les garanties procédurales dont bénéficient les suspects ou les personnes poursuivies. Dans le cadre des nouvelles évolutions technologiques mentionnées plus haut, lorsque le lieu où les données sont stockées n'est pas stable, le principe fondamental de la territorialité, qui détermine l'établissement de la compétence dans une procédure pénale, semble perdre de sa pertinence et crée des difficultés qui nuisent au bon déroulement de la procédure pénale.

22. Dans certains cas, une recherche licite dans le système de départ localisé sur le territoire dans le ressort duquel se déroule l'enquête pénale pourrait s'étendre à un système d'information connecté situé à l'étranger sans que l'on s'en rende compte ou sans que l'on sache précisément sur quel territoire le système d'information est situé. Cette situation peut déboucher en pratique sur un accès transfrontière "sans consentement" à des données stockées dans le ressort territorial d'un pays étranger, ce qui va au-delà des possibilités légales existantes (par exemple l'article 32, point b, de la convention du Conseil de l'Europe sur la cybercriminalité). Le traitement et l'utilisation des données extraites de cette manière sont régis par la législation nationale et sont soumis par conséquent à différentes normes de garanties procédurales.

---

[11] Voir le rapport du groupe du Conseil de l'Europe sur l'accès transfrontalier, du 6 décembre 2012, intitulé "Compétence et accès transfrontalier: quelles solutions? http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

23. La "disparition du lieu" peut se traduire par des demandes concurrentes aux fins de poursuites ou par des enquêtes parallèles, ce qui souligne une fois encore la nécessité d'associer les autorités judiciaires à un stade précoce, mais aussi de revoir les règles régissant l'établissement de la compétence et de se pencher sur les approches qui pourraient se substituer à la procédure d'entraide judiciaire, l'objectif étant de trouver une solution pour les situations dans lesquelles la localisation des données n'est pas connue, par exemple en cas d'accès transfrontière à des données aux fins de la justice pénale.

6. Recevabilité des preuves électroniques

24. Eurojust fait observer qu'en vertu des législations nationales, il se peut que les autorités judiciaires doivent évaluer soigneusement, sur la base de critères fixés par la loi, la légalité de la collecte des preuves, comme condition de leur recevabilité devant une juridiction, contrairement à ce qui se passe avec les modèles juridiques basés sur le principe de confiance, dans le cadre desquels toutes les preuves sont présentées et appréciées librement par le juge. Ces exigences doivent être prises en compte lors de la collecte et de la communication de preuves électroniques. Il se pourrait donc, par exemple, que les autorités compétentes soient tenues d'obtenir et réunir des preuves conformément aux exigences de systèmes judiciaires étrangers.

25. Une interprétation correcte de preuves électroniques dans une procédure pénale peut nécessiter un savoir-faire dont ne disposent peut-être pas en suffisance les parquets ou les juridictions. Par ailleurs, afin que les preuves électroniques soient correctement présentées dans une procédure judiciaire, il peut s'avérer nécessaire que les acteurs du système judiciaire soient sensibilisés aux questions de police scientifique, ce qui pourrait ne pas toujours être le cas.

26. Compte tenu de ce qui précède, une réflexion pourrait être engagée sur la sensibilisation, le partage des informations, l'échange de bonnes pratiques et la formation ciblée.

7. Appréciation au regard des droits fondamentaux et de l'État de droit

27. Des garanties procédurales effectives, des garanties en matière de protection des données et un respect scrupuleux de l'État de droit forment le socle commun sur la base duquel les initiatives stratégiques et les solutions pratiques visant à rendre les procédures pénales plus efficaces devraient être conçues.

28. Ainsi, il convient, systématiquement, de mettre soigneusement en balance les besoins des systèmes de justice pénale dans les procédures liées à la cybercriminalité, d'une part, et les principes établis en matière de droits fondamentaux, d'autre part. C'est une tâche difficile. Ces difficultés ont été rencontrées dans le cadre des travaux menés par le Conseil de l'Europe concernant un protocole additionnel sur l'accès transfrontière aux données. C'est ce qu'il ressort aussi d'une série d'arrêts rendus récemment par la Cour de justice européenne, dans lesquelles celle-ci a clairement indiqué au législateur que son travail devrait être inspiré par des considérations liées aux droits fondamentaux et à l'État de droit et systématiquement apprécié à l'aune de ces considérations.