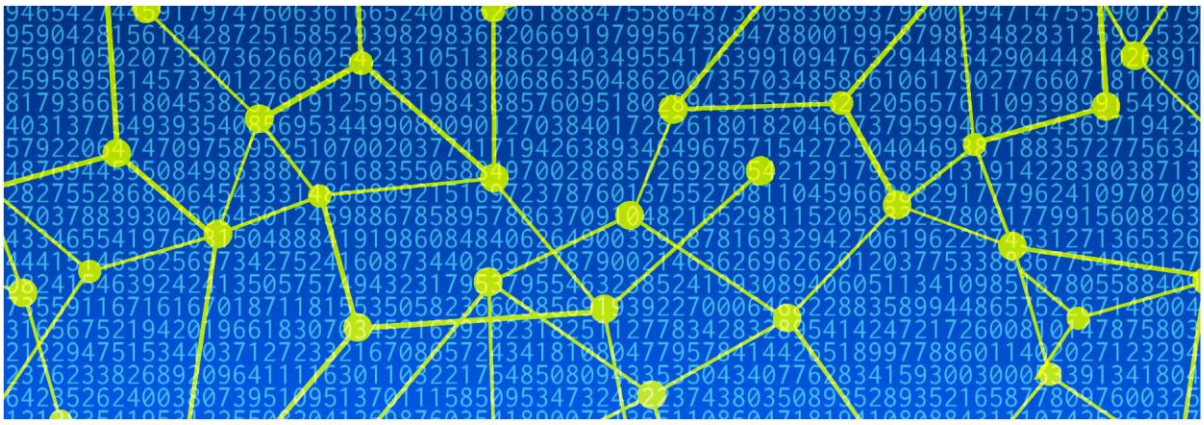

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 5/2019

concernant la révision des règlements de l'Union européenne relatifs à la signification ou à la notification des actes et à l'obtention des preuves en matière civile ou commerciale

13 septembre 2019

Le Contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union chargée, en vertu de l'article 52, paragraphe 2, du règlement (UE) 2018/1725, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment le droit à la protection des données, soient respectés par les institutions et organes de l'Union», et en vertu de l'article 52, paragraphe 3, «[...] de conseiller les institutions et organes de l'Union et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». En vertu de l'article 57, paragraphe 1, point g), du règlement (UE) 2018/1725, le CEPD «conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel».

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec pour mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis fournit des conseils sur deux propositions présentées par la Commission de révision des règlements relatifs à la signification ou à la notification des actes et à l'obtention des preuves en matière civile ou commerciale, notamment en ce qui concerne l'utilisation d'un système informatique à ces fins.

Synthèse

Le 31 mai 2018, la Commission européenne a publié deux propositions: d'une part, une proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention des preuves en matière civile ou commerciale; d'autre part, une proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 1393/2007 du Parlement européen et du Conseil relatif à la signification et à la notification dans les États membres des actes judiciaires et extrajudiciaires en matière civile et commerciale. Ces deux propositions visent principalement à améliorer le bon fonctionnement de la coopération judiciaire dans ces domaines, notamment en prévoyant la transmission des actes et l'obtention des preuves au moyen d'un système informatique décentralisé.

Le CEPD reconnaît que les échanges de données à caractère personnel sont nécessaires à la création d'un espace de liberté, de sécurité et de justice. Par conséquent, il se félicite des objectifs généraux des propositions visant à améliorer l'efficacité de la coopération judiciaire en matière civile ou commerciale en ce qui concerne l'obtention des preuves et la signification ou notification des actes, notamment grâce à la numérisation et à l'utilisation des technologies informatiques. Il partage le point de vue selon lequel la législation proposée pourrait avoir une incidence réelle sur la vie quotidienne des citoyens de l'Union.

Le CEPD formule trois recommandations principales afin d'aider de manière constructive les législateurs à atteindre cet objectif très important tout en garantissant le respect de la charte et du règlement général sur la protection des données (RGPD):

- définir une base juridique claire pour le système informatique qui serait utilisé pour la transmission des actes, demandes et communications aux fins de ces règlements. En particulier, dans le cas où le système informatique impliquerait la participation d'une institution, d'un organe ou organisme de l'Union, cette base juridique devrait en principe être prévue dans un acte législatif de l'Union. En outre, même dans le cas où le traitement des données à caractère personnel se ferait dans le cadre d'un système informatique existant, le CEPD recommande de prévoir l'utilisation d'un tel système dans l'acte législatif en question. Toutefois, le système existant dont l'utilisation est envisagée devrait lui-même être dûment établi sur la base d'un acte juridique adopté au niveau de l'Union, ce qui n'est pas le cas actuellement pour e-CODEX. Si le législateur de l'Union devait opter pour la solution e-CODEX, l'absence d'un instrument juridique au niveau de l'Union instaurant et réglementant le système devrait être comblée sans délai;

- inclure dans les actes législatifs en question une description détaillée des différents éléments du système informatique, tels que les responsabilités en matière de protection des données ou les mesures de protection applicables en la matière, à définir plus précisément dans les actes d'exécution. En particulier, dans la mesure où la Commission ou une autre institution, un autre organe ou organisme de l'Union participerait au fonctionnement du nouveau système, l'acte juridique devrait de préférence définir ses responsabilités en tant que responsable (conjoint) du traitement ou sous-traitant;

- réaliser une analyse d'impact relative à protection des données lors de l'élaboration des actes d'exécution.

Le CEPD formule d'autres recommandations détaillées dans le présent avis.

Le CEPD se tient à la disposition des institutions pour fournir tout conseil complémentaire au cours du processus législatif et lors de la phase d'exécution des règlements une fois ceux-ci adoptés.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1],

vu le règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE[2], et en particulier l'article 42, paragraphe 1, l'article 57, paragraphe 1, point g), et l'article 58, paragraphe 3, point c), de celui-ci,

A ADOPTÉ L'AVIS SUIVANT:

1. Introduction et contexte

1. Le 31 mai 2018, la Commission a adopté deux propositions[3] de règlements du Parlement européen et du Conseil visant à modifier:

   – le règlement (CE) nº 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'**obtention des preuves en matière civile ou commerciale** (ci-après le «règlement relatif à l'obtention des preuves»);

   – le règlement (CE) nº 1393/2007 du Parlement européen et du Conseil du 13 novembre 2007 relatif à la **signification et à la notification dans les États membres des actes judiciaires et extrajudiciaires en matière civile ou commerciale** (ci-après le «règlement relatif à la signification ou notification des actes»).

2. Le règlement relatif à l'obtention des preuves, qui s'applique depuis 2004, prévoit deux modes d'obtention des preuves entre les États membres: l'obtention des preuves par la juridiction requise et l'obtention directe des preuves par la juridiction requérante.

3. Le règlement relatif à la signification ou notification des actes, qui s'applique depuis 2008, prévoit différents modes de transmission des actes d'un État membre à un autre, aux fins de la signification ou notification dans ce dernier, par l'intermédiaire des entités d'origine et requises ou par voie consulaire ou diplomatique. Il fixe également des conditions juridiques uniformes pour la signification ou notification d'un acte par l'intermédiaire des services postaux directement à travers les frontières et prévoit une signification ou notification directe par l'intermédiaire de la personne compétente de l'État membre requis lorsque la législation de cet État membre le permet. Il comprend certaines normes minimales relatives à la protection des droits de la défense. L'application du règlement «*n'est pas limitée aux procédures devant les tribunaux civils, son champ d'application couvrant aussi les actes "extrajudiciaires", dont la signification ou la notification peut*

avoir lieu dans le cadre de différentes procédures extrajudiciaires (par exemple dans les affaires de succession devant un notaire ou dans les affaires relevant du droit de la famille devant une autorité publique), ou même en l'absence de toute procédure judiciaire sous-jacente»[4].

4. Les propositions figurent dans le programme de travail de la Commission pour 2018, sous la section Initiatives REFIT dans l'espace de justice et de droits fondamentaux basé sur la confiance mutuelle[5]. Les propositions sont accompagnées d'une analyse d'impact[6].

5. Les deux propositions prévoient la transmission des actes, demandes et communications au moyen d'un système informatique décentralisé obligatoire constitué de systèmes informatiques nationaux reliés entre eux par une infrastructure de communication permettant un échange transfrontalier d'informations sûr et fiable entre les systèmes informatiques nationaux. Elles prévoient également l'application du règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[7].

6. Le 13 février 2019, le Parlement européen a adopté en première lecture ses résolutions législatives sur les deux propositions[8]. Il s'est notamment accordé sur l'établissement d'un système informatique décentralisé qui soit fondé sur e-CODEX et dont la mise en œuvre soit garantie par des actes délégués.

7. Le 6 juin 2019, un débat d'orientation a eu lieu au sein du Conseil. La présidence a conclu que «*le Conseil avait confirmé la nécessité de moderniser nos processus dans le domaine de la coopération judiciaire en matière civile et commerciale. La présidence a noté la préférence exprimée en faveur d'un système informatique décentralisé et sûr. Elle a ajouté que les ministres ont pu accepter l'utilisation obligatoire du système uniquement à certaines conditions, parmi lesquelles une période de transition plus longue et une solution de référence devant être fournie par la Commission pour un système dorsal. Il conviendra aussi de réfléchir à une liste des exceptions nécessaires. Enfin, la présidence a noté qu'e-CODEX pourrait être la solution logicielle à retenir à cette fin. Les travaux devront se poursuivre au niveau technique*[9]».

8. Le 23 avril 2019, la Commission a adressé une demande de consultation au Contrôleur européen de la protection des données (ci-après le «CEPD») afin d'évaluer la conformité des deux propositions avec le règlement général sur la protection des données (ci-après le «RGPD»). Le CEPD se félicite de la consultation demandée par la Commission.

2. Recommandations

2.1. Base juridique

9. Le CEPD reconnaît que les échanges de données à caractère personnel sont indispensables à la création d'un espace de liberté, de sécurité et de justice. Par conséquent, il se félicite des objectifs généraux des propositions visant à améliorer l'efficacité de la coopération judiciaire en matière civile ou commerciale en ce qui concerne l'obtention des preuves et la signification ou notification des actes, notamment grâce à la numérisation et à l'utilisation des technologies informatiques. Il partage le point de vue selon lequel une telle législation peut avoir une incidence réelle sur la vie quotidienne des citoyens de l'Union.

10. Le CEPD rappelle que tout établissement d'un nouveau système informatique de traitement des données à caractère personnel ainsi que ses éléments essentiels nécessitent une base juridique[10]. Il souligne en particulier que **lorsqu'un tel système informatique implique la participation d'une institution, d'un organe ou d'un organisme de l'Union, cette base juridique devrait en principe être prévue dans un acte législatif de l'Union**.

11. En outre, même dans le cas où le traitement des données à caractère personnel se ferait dans le cadre d'un système informatique existant, le **CEPD recommande de prévoir l'utilisation d'un tel système dans l'acte législatif en question. Toutefois, le système existant dont l'utilisation est envisagée devrait lui-même être dûment établi sur la base d'un acte juridique adopté au niveau de l'Union, ce qui n'est pas le cas actuellement pour e-CODEX. Si le législateur de l'UE devait opter pour la solution e-CODEX, l'absence d'un instrument juridique au niveau de l'Union instaurant et réglementant le système devrait être comblée sans délai**.

2.2. Actes législatifs

12. **Le CEPD recommande d'inclure dans les actes législatifs une description détaillée des différents éléments du système informatique à définir plus précisément dans les actes d'exécution.** Ces éléments, fondés sur une évaluation des risques pour les droits fondamentaux des personnes physiques, devraient couvrir au moins les responsabilités en matière de protection des données (c'est-à-dire les rôles de responsable du traitement, de responsable conjoint du traitement et de sous-traitant, selon le cas) ainsi que les mesures de protection applicables en la matière, y compris celles garantissant la sécurité des données à caractère personnel traitées. Le respect de la protection des données n'est pas seulement une obligation légale, mais aussi un élément clé de l'efficacité du système envisagé, par exemple en garantissant la qualité des échanges de données.

2.2.1. Principes de la protection des données dès la conception et par défaut

13. L'exposé des motifs des deux propositions souligne que «[d]*'importants facteurs externes concernant la protection des données à caractère personnel dans le cadre du paquet de mesures proposé sont: – le règlement général sur la protection des données (RGPD), appliqué depuis mai 2018, qui devrait accroître la prise de conscience et pousser à agir pour garantir la sécurité et l'intégrité des bases de données et la rapidité de réaction aux atteintes à la vie privée au sein de l'appareil judiciaire;(...)»*[11]. Étant donné que le RGPD s'applique au traitement des données à caractère personnel aux fins de la coopération judiciaire en matière civile ou commerciale en vertu des deux règlements, le CEPD recommande d'appliquer ses principes dès le stade de l'établissement du système informatique, en particulier **les principes de protection des données dès la conception et par défaut** énoncés à l'article 25 du RGPD.

14. À cet égard, le **CEPD se félicite de la définition d'une architecture de haut niveau du système dans les actes législatifs en question et de l'obligation d'un échange fiable d'informations, ainsi que de la nécessité d'utiliser des services de confiance tels qu'ils sont définis dans le règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE**[12]. Il rappelle que le choix de l'architecture du système informatique permettant de réduire au minimum l'incidence sur la protection des données devrait reposer sur une évaluation des risques pour les personnes physiques dont les données sont traitées,

plutôt que sur l'architecture permettant de réduire au minimum les responsabilités éventuelles des États membres ou des institutions de l'Union. À moins d'un besoin spécifique de fonctionnalités centralisées, une architecture décentralisée pourrait permettre en effet, d'une manière générale, d'éviter les points uniques de défaillance et de soutenir le principe de réduction des données au minimum,

15. L'exposé des motifs des deux propositions souligne que l'autre facteur externe important à prendre en considération est «*les menaces persistantes pour la cybersécurité dans le secteur public. Les tentatives d'attaques visant les infrastructures informatiques publiques devraient se multiplier et affecter le système judiciaire dans les États membres; leur incidence peut être exacerbée par l'interconnexion croissante des systèmes informatiques (au niveau national et au niveau de l'UE)*»[13]. Il est extrêmement important que les données traitées dans ce système informatique soient protégées contre d'éventuels auteurs d'attaques et incidents de sécurité. En particulier, en ce qui concerne la **proposition relative à l'obtention des preuves, le CEPD recommande d'être plus précis quant aux mesures de protection appropriées requises pour garantir la sécurité de la vidéoconférence[14].** Ces mesures de protection devraient être précisées dans l'acte d'exécution (voir section 2.3. ci-dessous).

2.2.2. Définition des responsabilités

16. Le CEPD souligne que le choix d'une architecture décentralisée implique automatiquement que les États membres sont responsables des bases de données des actes de l'état civil ou commerciaux et du traitement des données à caractère personnel dans ces bases de données. Plus précisément, les autorités des États membres sont chargées du contrôle des bases de données des actes dont elles sont responsables. À ce titre, elles sont responsables du contenu des bases de données et de l'intégrité des informations échangées. Il est essentiel de veiller à ce que les responsabilités en matière de respect des règles de protection des données soient clairement définies et réparties.

17. Alors que les propositions visent à établir une architecture de haut niveau pour le système informatique envisagé, elles ne définissent pas la gouvernance ni les rôles et responsabilités de haut niveau des États membres et de la Commission (le cas échéant). Ces rôles et responsabilités sont toutefois essentiels à l'attribution du rôle de responsable du traitement et des obligations pertinentes en vertu de la législation applicable en matière de protection des données. Dans la mesure où la Commission ou une autre institution, un autre organe ou organisme de l'Union participerait au fonctionnement du nouveau système, l'acte juridique devrait de préférence définir ses responsabilités en tant que responsable (conjoint) du traitement ou sous-traitant. **Par conséquent, le CEPD recommande vivement de définir la gouvernance ainsi que les rôles et responsabilités de haut niveau des États membres et de la Commission ou de toute autre institution, de tout autre organe ou organisme de l'Union (le cas échéant) dans l'acte législatif.** Dans le cas où la Commission ou toute autre institution, tout autre organe ou organisme de l'Union aurait un rôle à jouer dans le traitement de ces données, le règlement (UE) 2018/1725 s'appliquerait à ce traitement.

18. En cas de responsabilité conjointe du traitement, les obligations de l'article 26 du RGPD ou de l'article 28 du règlement (UE) 2018/1725 s'appliqueraient, et la **relation entre les responsables conjoints du traitement et le contenu des dispositions obligatoires entre eux devraient être définis dans les actes d'exécution**.

2.3. Actes d'exécution

19. Le CEPD note que seule la proposition relative à la signification ou notification des actes prévoit l'adoption d'un acte d'exécution pour l'établissement du système informatique décentralisé[15]. **Par conséquent, il recommande de prévoir un tel acte d'exécution dans les deux propositions.**

20. Ces actes d'exécution devraient définir de manière plus détaillée les éléments importants du système. Ils devraient également contribuer à garantir le respect des exigences en matière de protection des données en précisant les mesures de protection nécessaires à mettre en œuvre dans le système informatique. En conséquence, **le CEPD recommande de prévoir dans les actes législatifs que l'acte d'exécution couvre également les nouvelles dispositions relatives à la signification ou notification électronique des actes[16] et à l'exécution directe de l'acte d'instruction par vidéoconférence[17]**.

21. Étant donné que les analyses d'impact accompagnant les propositions ne contiennent aucune analyse approfondie de l'incidence de ces propositions sur la protection des données, le **CEPD recommande vivement à la Commission de procéder à une analyse d'impact lors de l'élaboration des actes d'exécution**. Cela est sans préjudice des obligations qui incombent aux responsables du traitement en vertu du RGPD et, le cas échéant, du règlement (UE) 2018/1725, de réaliser en particulier une analyse d'impact relative à la protection des données en application de l'article 35 du RGPD ou de l'article 39 du règlement (UE) 2018/1725, si les conditions sont remplies[18].

22. En outre, d'après l'exposé des motifs des deux propositions[19], le CEPD comprend que le futur système informatique pourrait être le même pour les deux et que son accès serait limité à des utilisateurs spécifiques: pour la proposition relative à l'obtention des preuves, le nombre d'utilisateurs serait limité aux juridictions[20], aux autorités centrales et aux autorités compétentes au sens du règlement, telles qu'elles sont communiquées par les États membres, tandis que pour la proposition relative à la signification ou notification des actes, le nombre d'utilisateurs serait limité aux entités d'origine et requises[21] ainsi qu'aux organes centraux désignés par les États membres. Le CEPD **recommande que des mesures de protection garantissant l'accès à un nombre limité d'utilisateurs autorisés soient spécifiées dans les actes d'exécution**.

23. Enfin, les propositions introduiraient un nouvel article 23 *bis* dans le règlement relatif à la signification ou notification des actes et un nouvel article 22 *bis* dans le règlement relatif à l'obtention des preuves, en vertu desquels les États membres fournissent à la Commission les données et autres éléments de preuve nécessaires au programme de suivi que la Commission établit deux ans après la date de mise en application de ces règlements. Le CEPD comprend que ces programmes de suivi impliqueraient la collecte de données statistiques[22] et **recommande que les éléments statistiques à collecter soient définis de manière aussi détaillée que possible dans les actes d'exécution**.

3. Conclusions

24. Le CEPD se félicite des objectifs généraux des propositions visant à améliorer l'efficacité de la coopération judiciaire, notamment grâce à la numérisation et à l'utilisation des technologies informatiques, en ce qui concerne l'obtention des preuves ainsi que la

signification ou notification des actes en matière civile ou commerciale. Par conséquent, le présent avis vise à fournir des conseils constructifs et objectifs aux institutions de l'Union.

25. Le CEPD se félicite de la définition d'une architecture de haut niveau du système dans l'acte législatif en question et de l'obligation d'un échange fiable d'informations, ainsi que de la nécessité d'utiliser des services de confiance tels qu'ils sont définis dans le règlement (UE) nº 910/2014.

26. Le CEPD formule trois recommandations principales pour garantir le respect de la charte et du RGPD:

- définir une base juridique claire pour le système informatique qui serait utilisé pour la transmission des actes, des demandes et des communications aux fins de ces règlements. En particulier, dans le cas où le système informatique impliquerait la participation d'une institution, d'un organe ou d'un organisme de l'Union, cette base juridique devrait en principe être prévue dans un acte législatif de l'Union. En outre, même dans le cas où le traitement des données à caractère personnel se ferait dans le cadre d'un système informatique existant, le CEPD recommande de prévoir l'utilisation d'un tel système dans l'acte législatif en question. Toutefois, le système existant dont l'utilisation est envisagée devrait lui-même être dûment établi sur la base d'un acte juridique adopté au niveau de l'Union, ce qui n'est pas le cas actuellement pour e-CODEX. Si le législateur de l'Union devait opter pour la solution e-CODEX, l'absence d'un instrument juridique au niveau de l'Union instaurant et réglementant le système devrait être comblée sans délai;

- inclure dans les actes législatifs en question une description détaillée des différents éléments du système informatique, tels que les responsabilités en matière de protection des données ou les mesures de protection applicables en la matière, à définir plus précisément dans les actes d'exécution. En particulier, dans la mesure où la Commission ou un(e) autre institution, organe ou organisme de l'Union participerait au fonctionnement du nouveau système, l'acte juridique devrait idéalement définir ses responsabilités en tant que responsable (conjoint) du traitement ou sous-traitant;

- réaliser une analyse d'impact relative à la protection des données lors de l'élaboration des actes d'exécution.

27. Le CEPD formule également les recommandations suivantes:

- prévoir dans les deux actes législatifs un acte d'exécution détaillant plus précisément le système informatique et prévoir que les actes d'exécution couvrent les nouvelles dispositions relatives à la signification ou notification électronique des actes et à l'exécution directe de l'acte d'instruction par vidéoconférence, afin d'inclure également des mesures de protection spécifiques pour ces opérations de traitement;

- en cas de responsabilité conjointe du traitement, définir la relation entre les responsables conjoints du traitement et le contenu des dispositions obligatoires entre eux dans les actes d'exécution;

- préciser les mesures de protection garantissant l'accès à un nombre limité d'utilisateurs autorisés dans les actes d'exécution;

- définir de manière aussi détaillée que possible les éléments statistiques à collecter dans les actes d'exécution.

28. Enfin, le CEPD reste à la disposition de la Commission, du Conseil et du Parlement européen pour fournir des conseils au cours des étapes ultérieures de ce processus. Les recommandations formulées dans le présent avis sont sans préjudice des observations supplémentaires que le CEPD pourrait faire ultérieurement, notamment si de nouveaux problèmes étaient soulevés. Il rappelle que, conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725, la Commission est tenue, lors de l'élaboration d'actes délégués ou d'actes d'exécution, de consulter le CEPD en cas d'incidence sur la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel Par conséquent, le CEPD espère être consulté ultérieurement sur les dispositions des projets d'actes d'exécution ou d'actes délégués à cet égard.

Bruxelles, le 13 septembre 2019

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] JO L 119 du 4.5.2016, p. 1.
[2] JO L 295 du 21.11.2018, p. 39 [ci-après le «règlement (UE) 2018/1725»].
[3] Proposition COM(2018) 378 final (ci-après la «proposition relative à l'obtention des preuves») et proposition COM(2018) 379 final (ci-après la «proposition relative à la signification ou notification des actes»).
[4] Exposé des motifs, p. 2.
[5] Programme de travail de la Commission pour 2018: un programme pour une Europe plus unie, plus forte et plus démocratique [COM(2017) 650 final du 24.10.2017], annexe II, points 10 et 11.
[6] Documents de travail des services de la Commission SWD(2018) 285 final et SWD(2018) 287 final.
[7] Exposé des motifs de la proposition relative à l'obtention des preuves (p. 3) et de la proposition relative à la signification ou notification des actes (p. 4): *"[S]i, en principe, rien n'empêche les États membres de passer à des modes de communication numériques, l'expérience passée et les prévisions de ce qui se passera sans intervention de l'UE montrent que les progrès seraient très lents et que, même lorsque les États membres prennent des mesures, l'interopérabilité ne peut pas être garantie sans un cadre régi par le droit de l'UE. L'objectif de la proposition ne peut être atteint de manière suffisante par les États membres et ne peut l'être qu'au niveau de l'Union.*»
[8] P8_TA(2019)0103 et P8_TA(2019)0104.
[9] Résultats de la session du Conseil (9970/19), p. 7, version provisoire disponible à l'adresse: https://data.consilium.europa.eu/doc/document/ST-9970-2019-INIT/fr/pdf
Selon le document de la présidence (9566/19), points 8 et 13, «*dans les analyses d'impact de la Commission accompagnant les deux propositions, e-CODEX est considéré comme étant le système informatique le plus adapté et le seul aisément disponible. Le développement d'un autre système décentralisé signifierait que les mêmes défis déjà rencontrés dans le cadre du développement de e-CODEX devraient être relevés de nouveau». «L'une des solutions existantes est e-CODEX, un système développé avec le soutien financier de l'UE par un consortium d'États membres pendant une période de près de dix ans. E-CODEX est actuellement utilisé pour ce qui suit: le système d'interconnexion des registres du commerce (BRIS); l'interconnexion des registres d'insolvabilité nationaux; le système d'échange de preuves numériques. Toutefois, dans la mesure où cela concerne des cas d'utilisation fondés sur une coopération volontaire, e-CODEX n'est pas encore mis en œuvre ni utilisé par l'ensemble des États membres. Dans ce contexte, au cours des discussions au sein du groupe, la Commission pourrait réfléchir au développement, pour les États membres dans lesquels il n'existe actuellement aucun système informatique gérant les procédures électroniques, d'une solution de référence pour la mise en œuvre d'un système dorsal au niveau national, pour autant qu'il y ait un soutien suffisamment fort et large des délégations en faveur de l'obligation de communiquer par voie électronique. Tous les systèmes devraient être techniquement interopérables et conformes au même ensemble de spécifications techniques (protocoles, normes, schémas XML et déroulement des travaux).*»
[10] Avis du CEPD du 22 février 2008 concernant la décision de la Commission du 12 décembre 2007 relative à la protection des données à caractère personnel dans le cadre de la mise en œuvre du Système d'information du marché intérieur (IMI) (2008/49/CE), JO C 270/1 du 25.10.2008, points 20, 21 et 22: «*Sur la base de la jurisprudence relative à la CEDH, la nature juridique des dispositions qui restreignent des droits fondamentaux ne devrait faire aucun doute: elles doivent figurer dans un instrument législatif fondé sur le traité CE et susceptible d'être invoqué en justice. Sinon, il existerait une incertitude juridique pour la personne concernée, celle-ci ne pouvant pas être sûre de pouvoir invoquer les règles devant un juge.*
21. La question de la sécurité juridique est d'autant plus cruciale que, en vertu du système établi par le traité CE, c'est aux juges nationaux qu'il incombera au premier chef de décider de la valeur qu'ils reconnaissent à la décision IMI — — ce qui pourrait déboucher sur des résultats dissemblables entre les divers États membres, voire au sein d'un même État membre. Cette incertitude juridique est inacceptable
22. En tout état de cause, l'absence de voie de droit (ou de sécurité à cet égard) serait contraire à l'article 6 de la CEDH, qui consacre le droit à un procès équitable, ainsi qu'à la jurisprudence relative à cet article. Le cas échéant, la Communauté ne respecterait pas les obligations que lui impose l'article 6 du traité sur l'Union européenne, en vertu duquel l'Union respecte les droits fondamentaux tels qu'ils sont garantis par la CEDH.»
[11] Proposition relative à l'obtention des preuves (p. 6) et proposition relative à la signification ou notification des actes (p. 9 et 10).
[12] JO L 257 du 28.8.2014, p. 73.
[13] Proposition relative à l'obtention des preuves (p. 6) et proposition relative à la signification ou notification des actes (p. 9 et 10).
[14] En cas d'utilisation de services de communications électroniques accessibles au public, les dispositions de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données

à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37) s'appliqueraient.

[15] Voir le nouvel article 18 *bis* introduit par l'article 1er, paragraphe 12, de la proposition relative à la signification ou notification des actes.

[16] Voir le nouvel article 15 *bis* introduit par l'article 1er, paragraphe 10, de la proposition relative à la signification ou notification des actes.

[17] Voir le nouvel article 17 *bis* introduit par l'article 1er, paragraphe 4, de la proposition relative à l'obtention des preuves.

[18] Voir également les lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679» du groupe de travail «Article 29» (WP 248 rév. 01), note de bas de page 21: «*Dans le cas d'une AIPD réalisée au stade de l'élaboration de la législation conférant une base juridique au traitement, un réexamen pourra être nécessaire avant le lancement des opérations, la législation adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il est possible que les détails techniques disponibles en ce qui concerne le traitement effectif soient insuffisants au moment de l'adoption de la législation, même si une AIPD a été effectuée. Dans de tels cas, il pourra s'avérer nécessaire d'effectuer une AIPD spécifique avant d'exécuter les activités de traitement proprement dites.*»
Voir également la publication du CEPD «Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments», p. 10: «[...] *même lorsqu'une AIPD IAPD a été réalisée dans le respect des normes du règlement au stade de la proposition de base juridique, un réexamen pourrait être nécessaire avant le lancement des opérations, la base juridique adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il n'est généralement pas vrai que tous les choix opérés dès la conception ayant une incidence sur la vie privée et la protection des données soient déjà déterminés par la base juridique. Dans la pratique, de telles AIPD prévues dans le cadre du processus législatif peuvent tout au plus constituer la première étape du processus de l'AIPD*».

[19] En ce qui concerne les mesures de numérisation proposées et leur incidence sur les droits fondamentaux, l'exposé des motifs de la proposition relative à l'obtention des preuves explique en outre que «*le système à mettre en place pour les échanges électroniques entre les juridictions désignées devrait comprendre une solution technique pleinement fiable et sûre, qui garantit l'intégrité et la confidentialité des données transmises. Un ensemble prédéfini d'utilisateurs du système (uniquement les juridictions et les autorités judiciaires des États membres) donne une garantie supplémentaire que les données à caractère personnel seront traitées de manière appropriée. De plus, le système devrait prévoir une structure décentralisée, permettant une communication directe entre ses extrémités et réduisant ainsi le risque en limitant au minimum le nombre de sous-traitants des données*» [p. 6. (soulignement ajouté)]. L'exposé des motifs de la proposition relative à la signification ou notification des actes souligne que: «*le passage proposé à la communication électronique devrait avoir une incidence sur la protection des données à caractère personnel (article 8 de la charte). La mise en œuvre technique et l'exploitation des infrastructures électroniques seraient déterminées et contrôlées par les États membres eux-mêmes, même si les infrastructures sont partiellement développées et financées au niveau de l'UE. Les infrastructures devraient être fondées sur une architecture décentralisée. Les exigences en matière de protection des données s'appliqueraient donc uniquement au niveau national pour les différentes procédures*» [p. 9. (soulignement ajouté)]. Il explique en outre qu'un tel système «*garantirait la sécurité des communications électroniques et de l'échange d'actes entre les utilisateurs du système informatique décentralisé et prévoirait l'enregistrement automatique de toutes les étapes de la procédure.* [Il] *prévoirait aussi des dispositifs de sécurité garantissant que seuls les participants habilités dont l'identité a été contrôlée peuvent utiliser le système*» (p. 8).

[20] Voir l'article 2, paragraphe 2, l'article 3 et l'article 22 du règlement relatif à l'obtention des preuves. Dans la proposition relative à l'obtention des preuves, il est proposé d'entendre par «juridiction» «toute autorité judiciaire d'un État membre qui est compétente pour procéder à des actes d'instruction conformément au présent règlement» (ajout d'un paragraphe 4 à l'article 1er du règlement) afin de préciser que ce terme désigne également par exemple les notaires publics s'ils sont habilités par leur législation nationale à procéder à des actes d'instruction (exposé des motifs, p. 8).

[21] Conformément à l'article 2 du règlement relatif à la signification ou notification des actes, ces entités sont les officiers ministériels, autorités ou autres personnes compétents pour transmettre les actes judiciaires ou extrajudiciaires aux fins de signification ou de notification dans un autre État membre et pour recevoir de tels actes en provenance d'un autre État membre. Elles sont désignées par les États membres. Les informations sont communiquées à la Commission et publiées au Journal officiel de l'Union européenne (voir l'article 23 du règlement et l'article 1er, paragraphe 3, de la proposition relative à la signification ou notification des actes, qui ajoute un nouvel article 3 *bis*, paragraphe 1).

[22] Voir la liste des indicateurs dans l'analyse d'impact de la proposition de règlement modifiant le règlement relatif à l'obtention des preuves (p. 40) et dans l'analyse d'impact de la proposition de règlement modifiant le règlement relatif à la signification ou notification des actes (p. 54).