

Déclaration



Déclaration 02/2021 relative aux nouveaux textes de dispositions du deuxième protocole additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest)

Adoptée le 2 février 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Le comité européen de la protection des données (EDPB) a adopté la déclaration suivante:

Remarques préliminaires et contexte de la déclaration de l'EDPB

Le comité européen de la protection des données (EDPB) et les autorités chargées de la protection des données au sein de l'Union européenne suivent de près la préparation du deuxième protocole additionnel à la convention de Budapest, et ont régulièrement contribué aux consultations organisées par le Conseil de l'Europe, comme la «conférence Octopus» annuelle. En novembre 2019, l'EDPB a également publié sa dernière contribution aux consultations relatives à un projet de deuxième protocole additionnel¹, y indiquant qu'il restait «*disponible pour d'autres contributions*» et qu'il invitait «*les autorités chargées de la protection des données à participer, à un stade précoce et de manière plus dynamique, à la préparation de ces dispositions particulières, dans le but de veiller à une compréhension et à une prise en considération optimales des garanties en matière de protection des données*»².

À la suite de la publication des nouveaux textes de dispositions du deuxième protocole additionnel à la convention de Budapest³, l'EDPB souhaite donc, une fois de plus, apporter une contribution éclairée

¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf

² L'EDPB maintient les avis et les recommandations formulés dans cette précédente contribution et juge opportun de réaffirmer les principes clés à la lumière des dernières évolutions qui se sont produites et du projet de nouvelles dispositions publié.

³ <https://www.coe.int/fr/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultations>

et constructive en vue de garantir que les aspects liés à la protection des données sont dûment pris en considération tout au long du processus de rédaction dudit protocole additionnel, compte tenu du fait que les réunions consacrées à sa préparation sont organisées à huis clos et que le mandat du comité de la convention sur la cybercriminalité (T-CY)⁴ ne prévoit pas la participation directe des autorités chargées de la protection des données à ce processus de rédaction.

En outre, l'EDPB considère que les dispositions susmentionnées sont susceptibles de se répercuter sur les conditions de fond et de forme concernant l'accès aux données à caractère personnel au sein de l'Union, notamment en raison de demandes émanant d'autorités de pays tiers, et qu'elles font ainsi également écho aux débats en cours à l'échelle de l'Union et aux initiatives législatives connexes qu'étudient actuellement les colégislateurs⁵. Il invite donc la Commission européenne et le Parlement européen, ainsi que les États membres et les parlements nationaux de l'Union, à veiller à ce que les négociations en cours fassent l'objet d'un examen attentif visant à garantir la cohérence parfaite entre le deuxième protocole additionnel envisagé et l'acquis de l'Union, notamment en matière de protection des données à caractère personnel.

Par le passé, les autorités de l'Union chargées de la protection des données ont déjà abordé la question de l'accès aux données à caractère personnel dans les différentes juridictions dans plusieurs avis et positions, et l'EDPB souhaite une nouvelle fois rappeler, notamment, les observations du groupe de travail «article 29» sur la question de l'accès direct des autorités répressives des pays tiers aux données stockées dans d'autres juridictions, comme le propose le projet d'éléments pour un protocole additionnel à la convention de Budapest sur la cybercriminalité⁶, ainsi que la déclaration de ce groupe sur les aspects liés à la protection des données et à la vie privée dans le cadre de l'accès transfrontière aux preuves électroniques⁷. Le contrôleur européen de la protection des données (CEPD) a publié l'avis 3/2019 concernant le mandat autorisant la Commission à participer aux négociations⁸, ainsi que l'avis 7/2019 concernant les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale⁹. Ces contributions reposent également sur l'avis 23/2018 de l'EDPB concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale¹⁰.

L'EDPB demeure pleinement attentif au fait que les cas où les autorités judiciaires et répressives sont confrontées à un «cas transfrontière» en ce qui concerne l'accès aux données à caractère personnel dans le cadre de leurs enquêtes peuvent constituer une réalité difficile, et il ne perd pas de vue l'objectif légitime consistant à renforcer la coopération internationale en matière de cybercriminalité et d'accès aux informations. Parallèlement, il rappelle qu'il convient de garantir la protection des données à caractère personnel et la sécurité juridique, ce qui concourt à l'objectif consistant à établir un système pérenne permettant le partage de ces données avec les pays tiers à des fins répressives

⁴ Mandat pour la préparation d'un projet de 2^e protocole additionnel à la convention de Budapest sur la cybercriminalité, adopté par la 17^e réunion plénière du T-CY le 8 juin 2017, T-CY (2017)3.

⁵ En particulier, mais pas uniquement, les discussions concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

⁶ Observations du groupe de travail «article 29» sur la question de l'accès direct des autorités répressives des pays tiers aux données stockées dans d'autres juridictions, comme le propose le projet d'éléments pour un protocole additionnel à la convention de Budapest sur la cybercriminalité, 5 décembre 2013.

⁷ Déclaration du groupe de travail «article 29» sur les aspects liés à la protection des données et à la vie privée dans le cadre de l'accès transfrontière aux preuves électroniques, 29 novembre 2017.

⁸ Avis 3/2019 du CEPD relatif à la participation aux négociations en vue d'un deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité.

⁹ Avis 7/2019 du CEPD concernant les propositions relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

¹⁰ Avis 23/2018 de l'EDPB du 26 septembre 2018 concernant les propositions de la Commission relatives aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale.

et qui soit pleinement compatible avec les traités et la charte des droits fondamentaux de l'Union. L'EDPD estime par ailleurs qu'il est essentiel d'intégrer la préparation du protocole additionnel dans le cadre des valeurs et des principes fondamentaux du Conseil de l'Europe, et notamment des droits de l'homme et de l'état de droit.

En ce qui concerne l'«accès transfrontière [direct] à des données stockées» au sens de l'article 32, point b), de la convention de Budapest, l'EDPB réaffirme notamment qu'un responsable du traitement des données ne peut normalement divulguer des données que sur présentation préalable d'une autorisation ou d'un mandat judiciaire ou de tout autre document justifiant la nécessité d'accéder aux données et renvoyant à la base juridique applicable à cet accès, présenté par une autorité nationale chargée de veiller à l'application de la législation conformément à sa législation nationale, qui spécifiera la finalité de la demande d'accès aux données.

Étant donné que la convention de Budapest ainsi que chacun de ses protocoles additionnels constituent des instruments internationaux contraignants, l'EDPB souligne que, conformément à la jurisprudence de la Cour de justice de l'Union européenne, les «obligations qu'impose un accord international ne sauraient avoir pour effet de porter atteinte aux principes constitutionnels du traité CE, au nombre desquels figure le principe selon lequel tous les actes communautaires doivent respecter les droits fondamentaux, ce respect constituant une condition de leur légalité»¹¹. Il est donc essentiel que les parties aux négociations représentant l'Union veillent à ce que les dispositions définies dans le protocole additionnel soient effectivement conformes à l'acquis de l'Union en matière de protection des données afin de garantir sa compatibilité avec les droits primaire et dérivé de l'Union.

Compte tenu du calendrier du processus de consultation, la présente contribution de l'EDPB sera axée sur une évaluation préliminaire des nouveaux textes des dispositions du deuxième protocole additionnel de la convention de Budapest n'ayant pas fait l'objet des précédentes consultations des parties intéressées:

- les équipes communes d'enquête et les enquêtes communes,
- la divulgation accélérée de données informatiques stockées en situation d'urgence,
- la demande d'informations concernant l'enregistrement d'un nom de domaine.

Une fois encore, l'EDPB comprend que des dispositions spéciales en matière de protection des données à caractère personnel sont encore en cours d'examen. Il reste disponible pour d'autres contributions et invite les autorités chargées de la protection des données à participer, à un stade précoce et de manière plus dynamique, à la préparation de ces dispositions particulières, dans le but de veiller à une compréhension et à une prise en considération optimales des garanties en matière de protection des données.

Projet de dispositions provisoires relatives aux équipes communes d'enquête et aux enquêtes communes (ECE) (article 3), à la demande d'informations concernant l'enregistrement d'un nom de domaine (article 6) et à la divulgation accélérée de données informatiques stockées en situation d'urgence (article 7)

¹¹ Voir arrêt de la Cour dans les affaires jointes C-402/05 P et C-415/05 P, Kadi/Conseil, ECLI:EU:C:2008:461, point 285.

Sur la base de son évaluation préliminaire, l'EDPB recommande d'examiner plus en détail le projet de dispositions provisoires en ce qui concerne les éléments cités ci-après.

L'EDPB constate que ni les demandes d'informations concernant l'enregistrement d'un nom de domaine ni les demandes de divulgation accélérée de données informatiques stockées en situation d'urgence ne sont contraignantes. Par ailleurs, les motifs de refus d'accéder à la demande ne sont pas clairement définis, et la possibilité de refuser de coopérer en invoquant le droit de l'État Partie requis, y compris les motifs de refus établis dans des traités d'entraide judiciaire, manque également de clarté¹². Il rappelle à cet égard que les conditions sous lesquelles les fournisseurs de services de communications électroniques ou l'entité fournissant des services d'attribution de noms de domaine sont tenus d'octroyer cet accès doivent être prévues par la loi, de sorte à garantir que le traitement repose sur une base juridique claire.

En outre, l'EDPB renvoie à sa précédente contribution pour rappeler que, sauf cas d'urgence dûment justifiée¹³, et à la lumière de la jurisprudence de la Cour¹⁴, il considère que le type d'autorités requérantes pouvant adresser une telle demande doit se limiter à un parquet, à une autorité judiciaire ou à une autre autorité indépendante. Il estime également que la collaboration systématique d'autorités judiciaires avec les parties requises est essentielle pour garantir un examen efficace de la conformité des demandes par rapport à la convention et veiller à l'application du principe de la double incrimination dans le domaine de la coopération judiciaire.

L'EDPB rappelle à cet égard que le principe de la double incrimination vise à fournir une garantie supplémentaire pour garantir qu'une partie ne peut pas s'appuyer sur l'assistance d'une autre partie pour appliquer une sanction pénale qui n'existe pas dans la législation de cette autre partie. Outre qu'elle garantit le respect des droits des personnes et une procédure régulière dans le cadre du mécanisme de coopération judiciaire envisagé, cette garantie en prévoit également une autre, essentielle, liée aux conditions procédurales d'accès aux données à caractère personnel de ces personnes. Comme il l'a déjà indiqué dans sa précédente contribution, en ce qui concerne la sécurité du traitement des données, l'EDPB invite le T-CY à envisager, à titre de garantie spéciale en matière de protection des données, un mécanisme permettant la notification immédiate des violations des données susceptibles de porter gravement atteinte aux droits et aux libertés des personnes concernées. Les violations de données à caractère personnel risqueraient en effet d'avoir divers effets délétères notables pour ces personnes.

En lien avec le projet de dispositions provisoires relatives à la demande d'informations concernant l'enregistrement d'un nom de domaine, l'EDPB souligne que ces informations contiennent des données à caractère personnel et que, par conséquent, tout instrument international définissant les conditions de fond et de forme à remplir pour accéder à ces informations doit, en ce qui concerne les parties qui sont membres de l'Union européenne, être conforme aux droits primaire et dérivé de cette dernière.

S'agissant du texte provisoire des dispositions relatives à la «divulgation accélérée de données informatiques stockées en situation d'urgence» (article 7), l'EDPB constate que, en fonction de la manière dont chaque partie l'applique, ces nouvelles dispositions risquent d'impliquer la divulgation directe de données relatives au contenu. Il observe en outre que l'État Partie requis peut exiger, après

¹² Par exemple, le projet d'article 6, paragraphe 2, fait mention de «conditions raisonnables prévues par le droit interne».

¹³ L'EDPB fait observer que la notion de «situation d'urgence» est utilisée dans le sens établi au paragraphe 1 du projet de disposition relative à l'entraide urgente et considère qu'il est possible de préciser et de formuler plus en détail la définition de ce type de situation.

¹⁴ Voir arrêt de la Cour dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, point 120.

la divulgation des données, qu'une demande d'entraide judiciaire en bonne et due forme lui soit soumise (article 7, paragraphe 5). Dans ce dernier cas cependant, les parties au protocole envisagé ne s'engagent pas à effacer les données ou à ne pas les utiliser à titre d'éléments de preuve lorsque, sur la base des informations complémentaires obtenues grâce à la demande d'entraide appropriée, les autorités requises concluent que les conditions n'étaient pas remplies pour divulguer les données. Les conséquences juridiques de la divulgation des données, une fois celles-ci transmises au pays requérant, semblent donc être laissées à l'appréciation du droit national de ce pays. Par conséquent, l'absence d'engagement au niveau du protocole entraîne le risque de priver cette disposition de tout effet protecteur en ce qui concerne le traitement des données à caractère personnel déjà divulguées.

Enfin, l'EDPB met en évidence l'exigence prévue par l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne¹⁵, selon laquelle toute limitation de l'exercice des droits et libertés reconnus par la Charte doit respecter le principe de proportionnalité et ne peut être apportée que si elle est nécessaire. Dès lors, pour être légal au regard du droit de l'Union, le projet de dispositions du protocole envisagé doit satisfaire à cette exigence, qui porte ainsi tant sur les données à caractère personnel présentes dans la demande que sur celles figurant dans la réponse à cette demande. **Par conséquent, l'EDPB est particulièrement préoccupé par le libellé du projet d'article 6, paragraphe 3, point c), et du point 13 du projet de rapport explicatif en lien avec cette disposition, qui semble laisser entendre que les pays tiers requérants qui sont parties au protocole envisagé ne sont vraisemblablement pas tenus de respecter le principe de proportionnalité lorsqu'ils adressent des demandes à un État membre de l'Union.** En outre, la possibilité prévue par ces dispositions d'invoquer le principe de proportionnalité à titre de motif de refus manque de clarté.

Il est également difficile de savoir si les parties sont liées par l'obligation de veiller, dans le cadre du protocole envisagé, aux conditions et aux garanties définies à l'article 15 de la convention de Budapest¹⁶. **L'EDPB recommande de préciser que les obligations prévues par l'article 15 de la convention de Budapest sont pleinement applicables dans le cadre de cette coopération transfrontière.**

Dispositions relatives aux garanties en matière de protection des données

L'EDPB juge essentiel que le texte provisoire publié soit complété par des dispositions particulières relatives aux garanties en matière de protection des données, lesquelles doivent ensuite être évaluées conjointement avec d'autres dispositions, dans le but de veiller à ce que le projet de protocole additionnel débouche sur un système durable permettant le partage de données à caractère personnel avec les pays tiers à des fins répressives qui soit pleinement compatible avec les traités et la charte des droits fondamentaux de l'Union.

Du fait qu'il établit des modalités procédurales d'accès aux données à caractère personnel, le projet de dispositions provisoires relatives à la demande d'informations concernant l'enregistrement d'un nom de domaine et à la divulgation accélérée de données informatiques stockées en situation d'urgence pourrait déjà avoir des répercussions sur le niveau de protection des données à caractère personnel et également nécessiter l'apport de modifications afin de veiller à l'application opérationnelle des garanties appropriées en matière de protection des données. **À cet égard, l'EDPB tient de nouveau à souligner la nécessité d'appliquer les garanties en matière de protection des**

¹⁵ Voir également article 8, paragraphe 2, de la convention européenne des droits de l'homme.

¹⁶ Voir, en particulier, article 6, paragraphe 4, entre crochets.

données à tout échange de données à caractère personnel dans le cadre du protocole envisagé¹⁷, notamment en ce qui concerne le transfert de données à caractère personnel¹⁸.

L'EDPB estime que les dispositions spécifiques relatives aux garanties en matière de protection des données doivent tenir compte de principes clés, et notamment de la licéité, de la loyauté et de la transparence, de la limitation des finalités, de la minimisation des données, de l'exactitude, de la limitation de la conservation ainsi que de l'intégrité et de la confidentialité. De même, il tient à souligner l'importance de veiller au respect des droits fondamentaux des personnes (droits d'accès, de rectification, et droit à l'effacement) – toute restriction étant limitée par le principe de proportionnalité – et de prévoir des possibilités de recours juridictionnel effectif pour les personnes concernées en cas de violations des garanties en matière de protection des données. L'exercice de ces droits nécessite également la notification à la personne concernée, du moins dès lors que cette notification n'est plus susceptible de compromettre l'enquête. Ces principes, droits et obligations sont également conformes à la version modernisée de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (convention 108+), à laquelle adhèrent également de nombreuses parties à la convention de Budapest sur la cybercriminalité. Conformément à la convention 108+, ils s'appliquent à toutes les autorités chargées du traitement des données de la partie requérante en vue de garantir le maintien de la protection. **L'EDPB renvoie à sa contribution à la consultation publique de 2019 pour plus d'informations concernant les exigences de l'Union en la matière¹⁹.**

L'EDPB rappelle l'importance d'associer les autorités chargées de la protection des données au processus de rédaction du protocole additionnel, et se tient prêt à contribuer à la préparation du texte provisoire des dispositions relatives aux garanties en matière de protection des données et à soutenir le T-CY dans cette tâche.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

¹⁷ L'article 6, paragraphe 4, semble restreindre l'application des garanties ainsi que celle de l'article 15 de la convention uniquement aux informations divulguées, à l'exclusion des données à caractère personnel figurant dans la demande.

¹⁸ D'après le point 9 du projet de rapport explicatif, cette disposition ne peut/devrait s'appliquer qu'au transfert de données à caractère personnel réalisé par les équipes communes d'enquête.

¹⁹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbcontributionbudapestconvention_en.pdf