EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices du CEPD portant sur l'évaluation du caractère proportionné des mesures limitant les droits fondamentaux à la vie privée et à la protection des données à caractère personnel

Table des matières

I. Objectif et mode d'utilisation des présentes lignes directrices

Inscrits dans la charte des droits fondamentaux de l'Union européenne (ci-après la «**charte**»), les **droits fondamentaux** constituent les **valeurs essentielles** de l'Union européenne, également consacrées dans le traité sur l'Union européenne (ci-après le «TUE»)[1]. Parmi ces droits figurent les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel inscrits aux articles 7 et 8 de la charte. Les institutions et les organes de l'UE sont tenus de respecter ces droits fondamentaux, notamment lors de la conception et de la mise en œuvre de nouvelles politiques ou de l'adoption de nouvelles mesures législatives. D'autres normes relatives aux droits fondamentaux jouent également un rôle prépondérant dans l'ordre juridique de l'Union, en particulier la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la «**CEDH**»)[2].

Les **conditions nécessaires à l'imposition de limitations éventuelles** à l'exercice des droits fondamentaux figurent parmi les caractéristiques les plus importantes de la charte, étant donné qu'elles déterminent **la mesure dans laquelle les droits peuvent être effectivement exercés**[3].

Les conditions de **nécessité** et de **proportionnalité** d'une mesure législative entraînant une limitation des droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sont une **double exigence** essentielle à laquelle doit satisfaire toute mesure proposée supposant un traitement de données à caractère personnel. Toutefois, s'assurer que **la protection des données** devient **partie intégrante du processus d'élaboration des politiques de l'Union européenne** ne nécessite pas uniquement de bien comprendre les principes exprimés dans le cadre juridique et dans la jurisprudence pertinente, mais également d'adopter une approche **pratique et créative** pour trouver les solutions à des problèmes complexes, dans un contexte aux priorités politiques souvent divergentes[4].

La **Cour de justice de l'Union européenne** (ci-après la «CJUE») a reconnu que la législation de l'Union doit fréquemment satisfaire **plusieurs objectifs d'intérêt public** qui peuvent parfois être contradictoires et nécessitent la recherche d'un **juste équilibre** entre les différents

[1] L'article 2 du TUE dispose que «[l]'Union est fondée sur les valeurs de respect de la **dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités**». En outre, l'article 6, paragraphe 1, du TUE reconnaît les **droits, les libertés et les principes énoncés dans la charte**, qui a la même valeur juridique que les traités (caractères gras ajoutés).

[2] L'article 6, paragraphe 3, du TUE dispose que «[l]es droits fondamentaux, tels qu'ils sont garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et tels qu'ils résultent des **traditions constitutionnelles communes aux États membres**, font partie du **droit de l'Union en tant que principes généraux**» (caractères gras ajoutés).

[3] L'article 52, paragraphe 1, de la charte dispose que «toute limitation de l'exercice des droits et libertés reconnus par la présente charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui».

[4] Voir le **document stratégique du 4 juin 2014, «Le CEPD en tant que conseiller des institutions de l'UE à l'égard des politiques et des législations: tirer profit de dix années d'expérience»**, consultable à l'adresse suivante: https://edps.europa.eu/data-protection/our-work/publications/papers/edps-advisor-eu-institutions-policy-and-legislation_fr.

intérêts publics et les droits fondamentaux protégés par l'ordre juridique européen[5]. Parmi ces droits et ces intérêts consacrés par la charte, on peut citer: le droit à la vie (article 2) et à l'intégrité de la personne (article 3); le droit à la liberté et à la sûreté (article 6); la liberté d'expression (article 11); la liberté d'entreprise (article 16); le droit de propriété, notamment la propriété intellectuelle (article 17); le droit d'accès aux documents (article 42).

Les présentes lignes directrices ont été élaborées afin d'**aider à déterminer si les mesures proposées sont conformes** au droit de l'Union en matière de protection des données. Elles ont été conçues dans le but de mieux équiper les décideurs politiques et les législateurs de l'Union chargés **d'élaborer ou d'étudier des mesures qui prévoient le traitement de données à caractère personnel** et limitent le droit à la protection de ces données et au respect de la vie privée. Elles visent à aider les décideurs politiques et les législateurs, une fois qu'ils ont défini les mesures qui ont une incidence sur la protection des données ainsi que les priorités et les objectifs de ces mesures, à trouver des solutions qui réduisent au maximum les conflits entre ces priorités tout en étant proportionnées.

Le CEPD souligne qu'il est de la responsabilité du législateur d'évaluer la proportionnalité d'une mesure. Par conséquent, les présentes lignes directrices n'entendent ni ne peuvent fournir une évaluation définitive de la proportionnalité, ou de l'absence de proportionnalité, de toute proposition de mesure spécifique. Elles proposent plutôt **une méthodologie pratique pas-à-pas** permettant d'évaluer la proportionnalité de nouvelles mesures législatives, avec des explications et des exemples concrets. Elles répondent à des demandes d'orientations émanant des institutions de l'Union relativement aux exigences particulières posées à l'article 52, paragraphe 1, de la charte.

Les lignes directrices **complètent** le «guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel» publié par le CEPD (ci-après le «**guide pour l'évaluation de la nécessité**»)[6] et approfondissent, sous l'angle des droits à la vie privée et à la protection des données à caractère personnel[7], les orientations déjà existantes concernant les limitations des droits fondamentaux, au moyen par exemple d'analyses d'impact et de contrôles de compatibilité, établies par la Commission

[5] Affaire C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, ECLI:EU:C:2008:54, point 68. Dans ses conclusions rendues dans les affaires jointes C-203/15 et C-698/15 (*Tele2 Sverige AB*, ECLI:EU:C:2016:572, point 247), l'avocat général Saugmandsgaard Øe a expliqué que «*[c]ette exigence de proportionnalité dans une société démocratique – ou proportionnalité "stricto sensu" – découle à la fois de l'article 15, paragraphe 1, de la directive 2002/58, de l'article 52, paragraphe 1, de la [c]harte et d'une jurisprudence constante. Selon cette jurisprudence constante, une mesure portant atteinte à des droits fondamentaux ne peut être considérée comme proportionnée que si les inconvénients causés* ***ne sont pas démesurés*** *par rapport aux buts visés*» (caractères gras ajoutés). Au paragraphe 248, il souligne également que l'exigence de proportionnalité dans cette affaire particulière de conservation d'une grande quantité de données «*ouvre ainsi un débat sur les valeurs devant prévaloir dans une société démocratique et, en définitive, sur le type de société dans lequel nous souhaitons vivre*».

[6] CEPD, «Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel», 11 avril 2017, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf.

[7] Dans les présentes lignes directrices, il sera souvent fait mention de la «protection des données» en référence à la fois au droit à la **vie privée** et au droit à la **protection des données à caractère personnel**. Il est important de souligner toutefois qu'il s'agit de deux droits distincts. À propos de la différence entre les deux, voir: https://edps.europa.eu/data-protection/data-protection_fr.

européenne, le Conseil de l'Union européenne et l'Agence des droits fondamentaux de l'Union européenne (ci-après la «FRA»)[8].

Ces lignes directrices ont pour ambition d'explorer plus en détail, au moyen notamment d'exemples concrets, les questions relatives à l'incidence des mesures envisagées sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel. Elles se concentreront entre autres sur l'**outil nº 24** de la «**boîte à outils pour une meilleure réglementation**» conçue par la Commission, ainsi que sur les «**orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission**».

L'EDPS constate que la protection des données à caractère personnel a acquis une importance accrue ces dernières années et est de plus en plus reconnue comme une dimension que le législateur doit prendre en considération dans tous les domaines politiques et dans le cadre de

Pour accompagner les efforts réalisés par la Commission pour prendre cette dimension essentielle en considération **de manière proactive**, **dès l'étape de la préparation de l'analyse d'impact**, il sera également fait référence, dans la partie opérationnelle des présentes lignes directrices, à la **terminologie utilisée dans le cadre de la méthodologie d'analyse d'impact de la Commission** (soit les termes «***facteurs***», «***causes***»,«***définition du problème***»,«***incidence***»).

En raison également de la complexité et des spécificités de cet exercice, le CEPD **est résolu et disposé à prêter assistance aux services de la Commission ainsi qu'à contribuer aux travaux d'analyse d'impact** en fournissant toutes les informations utiles relatives à la protection des données en tant que droit fondamental.

L'unité «Politique et consultation» du CEPD peut être contactée pour toute question relative aux présentes lignes directrices et à la manière d'évaluer l'incidence des actes législatifs sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel. À cette fin, vous pouvez contacter l'adresse électronique fonctionnelle de l'unité «Politique et Consultation: POLICY-CONSULT@edps.europa.eu.

[8] Voir **l'outil nº 24** relatif aux **«Droits fondamentaux et droits de l'homme» de la boîte à outils pour une meilleure réglementation réalisée par la Commission européenne**, disponible à l'adresse suivante: http://ec.europa.eu/smart-regulation/guidelines/tool_24_fr.htm
ainsi que l'analyse plus approfondie présentée dans le **document de travail des services de la Commission**, «**Orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission**», SEC(2011) 567 final, disponible en anglais à l'adresse suivante: http://ec.europa.eu/smart-regulation/impact/key_docs/docs/sec_2011_0567_en.pdf.
Voir également les **lignes directrices du Conseil relatives aux étapes nécessaires à la vérification de la compatibilité avec les droits fondamentaux, établies à l'intention des instances préparatoires du Conseil**, 5377/15, 20 janvier 2015, disponibles à l'adresse suivante:
https://www.consilium.europa.eu/media/30208/qc0214079frn.pdf
ainsi que le **Manuel élaboré par la FRA «Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale - Orientations»**, mai 2018, disponible à l'adresse: https://fra.europa.eu/fr/publication/2019/application-de-la-charte-des-droits-fondamentaux-de-lunion-europeenne-dans-le.
Ces documents couvrent l'ensemble des droits fondamentaux et font également référence à plusieurs exemples extraits de la jurisprudence de la CJUE et relatifs aux droits consacrés aux articles 7 et 8 de la charte.

toutes les initiatives de la Commission. Cet état de fait ne provient pas seulement d'une meilleure prise de conscience du public, mais également du fait que **le traitement des données** (qui jusqu'à récemment aurait pu paraître inoffensif) **est de plus en plus susceptible d'avoir une forte incidence sur la vie de tous les citoyens**.

Il est fondamental de rappeler que **la nécessité et la proportionnalité**, bien qu'elles soient étroitement liées (puisque la législation doit satisfaire aux deux conditions), constituent **deux critères différents**. Cette différence est manifeste dans la liste pratique des points à vérifier, étape par étape, pour évaluer la proportionnalité, présentée à la section III des présentes lignes directrices, et dans laquelle nous proposons la première vue d'ensemble de la **séquence globale des opérations.**

Les lignes directrices comprennent **la présente introduction**, qui définit le contenu et l'objectif du guide, une **analyse juridique** du critère de la proportionnalité appliqué au traitement des données à caractère personnel, ainsi qu'une **liste pratique des points à vérifier, étape par étape** pour évaluer la nécessité de toute nouvelle mesure législative. La liste des points à vérifier constitue l'élément central des lignes directrices et peut être utilisée de façon autonome.

Les lignes directrices sont fondées sur la **jurisprudence**[9] de la CJUE, de la Cour européenne des droits de l'homme (ci-après la «Cour EDH»), les avis du CEPD et du groupe de travail «article 29», ainsi que sur les lignes directrices du comité européen de la protection des données.

Par ces lignes directrices, associées au **guide pour l'évaluation de la nécessité**, nous avons pour ambition de proposer une **approche commune de l'évaluation du caractère nécessaire et proportionnel** des mesures législatives au regard des droits à la vie privée et à la protection des données à caractère personnel.

II. Analyse juridique: application du critère de la proportionnalité aux droits à la vie privée et à la protection des données à caractère personnel

1. Du **critère de la proportionnalité** dans le cadre de l'évaluation de la légalité de toute proposition de mesure prévoyant le traitement de données à caractère personnel

L'article 8 de la charte consacre le **droit fondamental à la protection des données à caractère personnel**. Ce droit n'est **pas absolu** et **peut être limité**, pourvu que les limitations respectent les exigences énoncées à l'article 52, paragraphe 1, de la charte. La même analyse s'applique au **droit au respect de la vie privée** consacré à l'article 7 de la charte[10].

[9]Pour un aperçu général de la **jurisprudence** pertinente de la CJUE et de la Cour EDH, voir le **Manuel de droit européen en matière de protection des données édité par la FRA**, édition 2018, disponible à l'adresse https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_fr.pdf.
Voir également la «fiche thématique - Protection des données personnelles» publiée en septembre 2018 par la Cour EDH, disponible à l'adresse https://www.echr.coe.int/Documents/FS_Data_FRA.pdf

[10] Dans ses conclusions rendues dans les affaires jointes C-92/09 et C-93/09 (*Volker und Markus Schecke* et *Hartmut Eifert*, ECLI:EU:C:2010:353, point 73), l'avocat général Sharpston a expliqué que *« [c]omme nombre des droits classiques protégés par la CEDH, le droit au respect de la vie privée **n'est pas un droit absolu**. L'article 8, paragraphe 2, de la CEDH admet expressément la possibilité de déroger à ce droit, tout comme*

Pour être légale, toute limitation de l'exercice des droits fondamentaux protégés par la charte doit respecter les **critères** suivants, tels qu'ils sont énoncés à l'article 52, paragraphe 1, de la charte:

- elle doit être **prévue par la loi**,
- elle doit **respecter le contenu essentiel** des droits,
- elle doit **répondre effectivement à des objectifs d'intérêt général** reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui,
- elle doit être **nécessaire** (c'est l'objet du guide pour l'évaluation de la nécessité), et
- elle doit être **proportionnée** (c'est l'objet des présentes lignes directrices).

Cette liste de **macro-critères** préfigure **l'ordre dans lequel l'évaluation** de la légalité d'une limitation de l'exercice d'un droit fondamental doit être menée.

1. Tout d'abord, il convient d'examiner si la loi qui prévoit la limitation est **accessible et prévisible**[11]**.** Si cette exigence n'est pas satisfaite, alors la mesure est illégale et il est

l'article 9 de la convention nº 108 s'agissant du droit à la protection des données à caractère personnel. De même, l'article 52 de la charte prévoit (en termes généraux) des conditions similaires, qui, si elles sont remplies, autorisent les exceptions (ou les dérogations) aux droits prévus par la charte» (caractères gras ajoutés). Cette approche a été confirmée par la CJUE aux points 48 à 50 de l'arrêt du 9 octobre 2010 (ECLI:EU:C:2010:662).

À propos du caractère «non absolu» du droit à la protection des données à caractère personnel, voir le considérant 4 du règlement (UE) 2016/679 (le «règlement général sur la protection des données», ci-après le «RGPD»): «Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le **droit à la protection des données à caractère personnel n'est pas un droit absolu**; il doit être considéré **par rapport à sa fonction dans la société** et **être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité**» (caractères gras ajoutés).

À propos de la différence entre **droits absolus** (tels que l'interdiction de la torture et des peines ou traitements inhumains ou dégradants, consacrée à l'article 4 de la charte) et **droits susceptibles d'être limités** (tels que le droit à la vie privée et à la protection des données à caractère personnel), voir la page 9 du document de travail des services de la Commission «Orientations opérationnelles concernant la prise en considération des droits fondamentaux dans les analyses d'impact réalisées par la Commission», SEC (2011) 567 final, ainsi que la page 70 du manuel de la FRA «Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale - Orientations», mai 2018.

Cette distinction emporte une conséquence importante: **les droits absolus ne sauraient être limités et, partant, ne peuvent être mis en balance avec d'autres droits ou d'autres intérêts**. Dès lors, dans les cas où le **droit à la vie privée et un droit absolu concordent** (vont dans la même direction; par exemple, le droit ne pas être soumis à la torture), **aucun des deux droits (concordants) ne peut être mis en balance** avec d'autres droits ou intérêts (tels que la sécurité nationale).

[11]L'article 52, paragraphe 3, de la charte de l'Union se lit comme suit: «Dans la mesure où la présente [c]harte contient des droits correspondant à des droits garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue.»

À propos de l'acception du terme «**prévu par la loi**» inscrit à l'article 52, paragraphe 1, de la charte, les critères développés par la Cour EDH devraient être interprétés de la manière suggérée dans les conclusions de plusieurs avocats généraux, notamment celles relatives aux affaires jointes C-203/15 et C-698/15 (*Tele2 Sverige AB*, ECLI:EU:C:2016:572, points 137-154) ainsi qu'à l'affaire C-70/10 (*Scarlet Extended*, ECLI:EU:C:2011:255, points 88-114). Dans le même ordre d'idées, voir, entre autres, l'arrêt de la Cour EDH dans l'affaire *Weber et Saravia c. Allemagne*, point 84: «La Cour rappelle que les mots "prévue par la loi", au sens de l'article 8, paragraphe 2 [de la CEDH], veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause: ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit.»

inutile de poursuivre son évaluation[12].

2. Deuxièmement, si la mesure a satisfait au critère de la qualité de la loi défini au point 1 ci-dessus, il convient de déterminer si **le contenu essentiel du droit** est respecté, c'est-à-dire si le droit ne se trouve pas, de fait, **vidé** de sa substance et si le justiciable peut bien l'exercer. S'il est porté atteinte au contenu essentiel du droit, la mesure est illégale et il est inutile de poursuivre l'évaluation de sa compatibilité avec les règles énoncées à l'article 52, paragraphe 1, de la charte[13].

Voir également le 41e considérant du RGPD: «Cette [base juridique ou cette] mesure législative devrait être **claire** et **précise** et son application devrait être **prévisible pour les justiciables**, conformément à la jurisprudence de la Cour de justice de l'Union européenne [...] et de la Cour européenne des droits de l'homme» (caractères gras ajoutés).

- Sur la notion de «**prévisibilité**» dans le cadre de l'**interception de communications**, voir l'affaire jugée par la Cour EDH, *Zakharov c. Russie*, point 229: «La Cour a jugé à plusieurs reprises que, en matière d'interception de communications, la "prévisibilité" ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence. Or le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes.» (caractères gras ajoutés). Toujours dans le même sens, très récemment, voir *Big Brother Watch e.a. c. Royaume-Uni*, Cour EDH, 13 septembre 2018, point 306.

- voir également l'affaire *Shimovolos c. Russie,* Cour EDH, 21 juin 2011.

[12] Voir l'affaire jugée par la Cour EDH, *Benedik contre Slovénie*, point 132: «la Cour estime que la mesure contestée, à savoir l'obtention par les services de police d'informations relatives aux abonnés associées à l'adresse IP dynamique en question [...], est fondée sur une loi rédigée en termes **insuffisamment clairs** et appliquée de manière tout aussi imprécise par les tribunaux nationaux; en outre, ladite mesure ne présente pas suffisamment de garanties contre toute ingérence arbitraire dans les droits consacrés à l'article 8. Dans ces circonstances, la Cour conclut que l'ingérence dans le droit du requérant au respect de sa vie privée n'était **pas «prévue par la loi»** au sens de l'article 8, paragraphe 2, de la convention. Partant, la Cour **n'est pas tenue d'examiner si la mesure contestée poursuivait un objectif légitime et était proportionnée**» (caractères gras ajoutés).

Voir également les affaires jointes *C-465/00, Rechnungshof/Österreichischer Rundfunk e.a., C-138/01, Christa Neukomm et C-139/01, Joseph Lauermann/Österreichischer Rundfunk*, ECLI:EU:C:2003:294, points 77-80; les conclusions de l'avocat général dans l'avis 1/15 de la Cour sur l'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens, ECLI:EU:C:2017:592, points 191-192: «*En ce qui concerne la conservation des données à caractère personnel, il y a lieu de relever que la réglementation en cause doit, notamment, toujours répondre à des critères objectifs, établissant un rapport entre les données à caractère personnel à conserver et l'objectif poursuivi (voir, en ce sens, arrêts du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 93, ainsi que du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 110). S'agissant de l'utilisation, par une autorité, de données à caractère personnel légitimement conservées, il convient de rappeler que la Cour a jugé qu'une réglementation de l'Union ne saurait se limiter à exiger que l'accès auxdites données réponde à l'une des finalités de cette réglementation, mais doit également* ***prévoir les conditions matérielles et procédurales régissant cette utilisation*** *(voir, par analogie, arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 117 et 118 ainsi que jurisprudence citée).*»

[13] Bien que la jurisprudence ne soit pas très abondante en ce qui concerne les conditions dans lesquelles il est porté atteinte au **contenu essentiel** d'un droit, l'on peut affirmer qu'il en irait autrement **si la limitation allait si loin qu'elle viderait le droit de ses éléments fondamentaux** et en empêcherait ainsi l'exercice.

- Dans l'affaire **C-362/14** (*Schrems*, ECLI:EU:C:2015:650, point 94, 95), la CJUE a conclu que **le contenu essentiel du droit au respect de la vie privée et du droit à un recours effectif** étaient affectés: «*une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la [c]harte [...]. De même, une réglementation* ***ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit*** *afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles*

3. Troisièmement, il convient de déterminer si la mesure répond à un **objectif d'intérêt général**. L'objectif d'intérêt général définit le **cadre** dans lequel la nécessité de la mesure peut être évaluée. C'est la raison pour laquelle, comme il est expliqué dans le guide pour l'évaluation de la nécessité, il est primordial de déterminer de façon suffisamment précise l'objectif d'intérêt général afin de pouvoir évaluer la nécessité de la mesure.

4. Il s'agit ensuite d'évaluer la **nécessité** de la mesure législative proposée qui prévoit le traitement de données à caractère personnel (critère de la nécessité)[14].

5. S'il est satisfait au critère de la nécessité, la **proportionnalité** de la mesure envisagée est évaluée (critère de la proportionnalité). Le concept de proportionnalité est un concept juridique bien établi par le droit de l'Union. Il s'agit **d'un principe général du droit de l'Union** en vertu duquel «*le contenu et la forme de l'action de l'Union* ***n'excèdent pas ce qui est nécessaire pour atteindre les objectifs*** *des traités*»[15] (caractères gras ajoutés). Il est fondé sur les traditions constitutionnelles de plusieurs États membres[16].

Aux termes de l'article 52, paragraphe 1, de la charte, «[d]ans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires [...]». Selon une jurisprudence constante de la CJUE, «*le principe de proportionnalité exige que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à*

---

données, ***ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle*** *effective, tel que consacré à l'article 47 de la charte*» (points 94 et 95) (caractères gras ajoutés). La Cour n'a pas poursuivi l'examen visant à déterminer si une telle limitation était nécessaire et a **déclaré invalide**, pour d'autres motifs également, **la décision de la Commission** relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité».

- Dans les affaires jointes **C-293/12 et C-594/12** (*Digital Rights*, ECLI:EU:C:2014:238, point 39), la CJUE a estimé qu'il n'était **pas porté atteinte** au **contenu essentiel du droit *au respect de la vie privée*** dans la mesure où la directive sur la conservation des données **ne permettait pas de prendre connaissance *du contenu*** des communications électroniques (mais uniquement de «métadonnées»).

Selon la CJUE, cette conservation des données n'était pas non plus de nature à porter atteinte au **contenu essentiel du droit à *la protection des données à caractère personnel*** puisque la directive sur la conservation des données prévoyait une **règle de base selon laquelle il convenait d'adopter des mesures techniques et organisationnelles appropriées contre la destruction, la perte ou l'altération accidentelles ou illicites des données** (point 39, 40). Ce n'est qu'après avoir déterminé que le contenu essentiel du droit fondamental en cause n'était pas compromis que la Cour a procédé à l'examen de **la nécessité** de la mesure.

- Dans les affaires jointes **C-203/15 et C-698/15** (*Tele2 Sverige AB,* ECLI:EU:C:2016:970, point 123), la Cour a estimé que la **privation de contrôle**, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union pourrait également **porter atteinte au contenu essentiel du droit à la protection des données à caractère personnel**, tel qu'il est explicitement exigé à l'article 8, paragraphe 3, de la charte et « *[s]'il en était autrement, les personnes dont les données à caractère personnel ont été conservées seraient privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs données*».

[14]Voir notre analyse du **critère de la nécessité** dans le guide pour l'évaluation de la nécessité du CEPD, disponible à l'adresse https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_fr.

[15] Voir l'article 5, paragraphe 4, du TUE.

[16] Le principe a été développé par la CJUE dans l'affaire *Internationale Handelsgesellschaft*, **C-11/70,** ECLI:EU:C:1970:114. À l'instar du droit administratif allemand, au niveau de l'Union européenne, le respect des critères de nécessité et de proportionnalité d'une mesure est vérifié en trois étapes: (i) la pertinence; (ii) la nécessité; et (iii) la proportionnalité *stricto sensu*. À cet égard, voir C. Bagger Tranberg, *Proportionality and data protection in the case law of the European Court of Justice*, International Data Privacy Law, 2011, Vol. 1, Nº 4, page 240.

la réalisation de ces objectifs»[17]. Par conséquent, **la proportionnalité au sens large** (à laquelle la CJUE fait référence) englobe **à la fois la nécessité** et **la pertinence** (**la proportionnalité dans son *sens restreint***) d'une mesure, c'est-à-dire la mesure dans laquelle il existe un lien logique entre la mesure et l'objectif (légitime) poursuivi[18].

Par ailleurs, pour qu'une mesure respecte le principe de proportionnalité inscrit à l'article 52, paragraphe 1, de la charte, **les avantages résultant de la mesure ne doivent pas être contrebalancés par les inconvénients** causés par la mesure au regard de l'exercice des droits fondamentaux. Par conséquent, ce principe «***limite les autorités*** *dans l'exercice de leurs pouvoirs en exigeant d'elles qu'elles* ***parviennent à un équilibre*** *entre les* ***moyens utilisés et l'objectif visé (ou le résultat atteint)***»[19].

En effet, dans l'arrêt *Digital Rights*[20], la CJUE a estimé que le **pouvoir d'appréciation du législateur** est réduit lorsqu'il s'agit de restreindre les droits fondamentaux: «*dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci*»[21]. Répondant sur le fond à la question «Quelle est **l'étendue du pouvoir d'appréciation (limité) du législateur de l'Union**?», la CJUE a déclaré: «*la réglementation de l'Union en cause* ***doit*** *prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*»[22] (caractères gras ajoutés).

---

[17] Affaire C-62/14, *Gauweiler (OMT)*, ECLI:ECLI:EU:C:2015:400, point 67. Voir également C-331/88, *Fedesa e.a.*, ECLI:EU:C:1990:391, point 13: *«En ce qui concerne le contrôle de proportionnalité, le principe de proportionnalité, qui fait partie des principes généraux du droit communautaire, exige que les actes des institutions communautaires ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation des objectifs légitimes poursuivis par la réglementation en cause, étant entendu que, lorsqu'un choix s'offre entre plusieurs mesures appropriées, il convient de recourir à la moins contraignante, et que les inconvénients causés ne doivent pas être démesurés par rapport aux buts visés»* .

[18] À titre d'exemple possible de ce qu'est la **proportionnalité au sens large**, englobant les critères de nécessité et de proportionnalité, voir C-594/12, *Digital Rights*, arrêt dans lequel la nécessité (§ 65: «*Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la [c]harte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au* ***strict nécessaire***.*»*) et la proportionnalité (§ 69: «*Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de* ***proportionnalité*** *au regard des articles 7, 8 et 52, paragraphe 1, de la [c]harte.*») sont examinés séparément par la CJUE. En d'autre termes, la CJUE s'exprime sur le principe de proportionnalité *après* avoir analysé la nécessité.

[19] K. Lenaerts, P. Van Nuffel, *European Union Law*, Sweet and Maxwell, 3e édition, Londres, 2011, p. 141 (affaire C-343/09, *Afton Chemical*, point 45; affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke et Hartmut Eifert*, EU:C:2010:662, point 74; affaires C-581/10 et C-629/10, *Nelson e.a.*, point 71; affaire C-283/11, *Sky Österreich*, point 50; et affaire C-101/12, *Schaible*, point 29).

[20] Affaires jointes C-293/12 et C-594/12, ECLI:EU:C:2014:238.

[21] Ibid., point 47.

[22] Ibid., point 54.

Voir également les pages 6 et 7 de **l'avis 5/2015 du CEPD intitulé «Deuxième avis sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers(PNR) pour la prévention et la détection des infractions terroristes et des formes graves de**

Ce dernier élément (l'équilibre à atteindre) décrit le **principe de proportionnalité au sens strict** et constitue le critère de la proportionnalité dont l'évaluation fait l'objet des présentes lignes directrices. Il doit être précisément distingué de la nécessité (voir la section III ci-dessous), à la fois d'un point de vue conceptuel et d'un point de vue pratique.

2. Précisions concernant **la relation** entre proportionnalité et nécessité

Comme il est précisé dans le guide pour l'évaluation de la nécessité, «**[l]e principe de nécessité suppose le besoin de procéder à une évaluation factuelle combinée de l'efficacité de la mesure aux fins de l'objectif poursuivi et de déterminer si cette mesure est moins intrusive par rapport aux autres moyens de réaliser le même objectif**». Le critère de la nécessité doit être considéré comme **la première étape** que doit franchir une proposition de mesure prévoyant le traitement de données à caractère personnel. Si ce critère n'est **pas satisfait**, il est alors **inutile d'en évaluer** la proportionnalité. Une mesure qui s'avère inutile ne doit pas être proposée tant qu'elle n'a pas été modifiée de façon à satisfaire à l'exigence de la nécessité: en d'autres termes, **la nécessité constitue une condition préalable du principe de proportionnalité**[23].

Les présentes lignes directrices partent par conséquent du postulat que seule une mesure s'avérant nécessaire peut faire l'objet d'un examen de la proportionnalité. Comme il est mentionné dans le guide pour l'évaluation de la nécessité, dans des affaires récentes, la CJUE **n'a pas procédé à l'examen de la proportionnalité** après avoir constaté que les limitations aux droits reconnus aux articles 7 et 8 de la charte **n'étaient pas** strictement nécessaires[24].

Toutefois, une fois que la mesure législative a été jugée **nécessaire**, il convient de l'examiner à l'aune du **principe de proportionnalité**. **Un examen de la proportionnalité suppose en règle générale de déterminer quelles «garanties» doivent accompagner une mesure** (qui porterait par exemple sur la surveillance) afin de réduire à un niveau «acceptable»/proportionné les risques posés par la mesure envisagée au regard des droits fondamentaux et des libertés des individus concernés.

---

criminalité, ainsi que pour les enquêtes et les poursuites en la matière»: «Dans le contexte de la réalisation d'un **test de proportionnalité**, la **mesure dans laquelle le pouvoir d'appréciation du législateur de l'Union peut s'avérer limité** est fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature des droits en cause, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci. La Cour a insisté sur le fait que ces limitations et garanties sont encore plus importantes lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données». L'avis du CEPD est disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_fr.pdf.

[23] Dans les affaires jointes **C-465/00, C-138/01 et C-139/01**, *Rechnungshof*, ECLI:EU:C:2003:294, § 91, la CJUE a estimé que: «*Si les juridictions de renvoi concluent à l'**incompatibilité** avec l'article 8 de la CEDH de la réglementation nationale en cause, cette dernière **ne peut pas satisfaire non plus à l'exigence de proportionnalité** énoncée aux articles 6, paragraphe 1, sous c), et 7, sous c) ou e), de la directive 95/46*» (caractères gras ajoutés).

[24] Dans les affaires jointes **C-293/12 et C-594/12** (*Digital Rights*, ECLI:EU:C:2014:238), la CJUE a tout d'abord indiqué que le principe de proportionnalité consistait à juger du caractère approprié et nécessaire de la mesure (point 46). Elle a ensuite établi que la limitation des droits protégés par les articles 7 et 8 n'était **pas nécessaire** (point 65) et en a, partant, conclu que les limitations n'étaient pas proportionnées (point 69).
De même, dans l'affaire **C-362/14** (*Schrems*, ECLI:EU:C:2015:650, points 92 et 93), après avoir procédé à l'examen de la nécessité, la Cour a déclaré invalide la décision sur les principes de la «sphère de sécurité», sans faire **la moindre référence au principe de proportionnalité** avant de parvenir à cette conclusion (point 98).

L'efficacité des mesures existantes par rapport à la proposition de mesure constitue également un autre élément à prendre en considération dans l'évaluation de la proportionnalité[25]. Si des mesures poursuivant un objectif similaire ou identique existent déjà, leur efficacité doit être systématiquement évaluée dans le cadre de l'examen de la proportionnalité. Faute d'avoir réalisé cette évaluation, il sera considéré que l'examen du critère de proportionnalité pour une nouvelle mesure n'a pas été dûment mené.

3. **Conclusion**: le principe de proportionnalité dans la législation relative à la protection des données: une notion factuelle qui requiert une évaluation au cas-par-cas du législateur de l'Union

L'«émergence d'une exigence de proportionnalité» est considéré comme l'«**un des développements les plus remarquables** de ces dix dernières années dans le domaine du droit européen de la protection des données»[26].

Le principe de proportionnalité a été ajouté à l'article 5, paragraphe 1, de la **convention 108 modernisée**[27], libellé ainsi: «Le traitement de données doit être **proportionné** à la finalité légitime poursuivie et refléter à chaque étape du traitement un **juste équilibre** entre tous les intérêts en présence, qu'ils soient publics ou privés, ainsi que les droits et les libertés en jeu» (caractères gras ajoutés).

La notion de proportionnalité repose sur le concept de **mise en balance**: il s'agit de mesurer l' **importance de l'ingérence** *par rapport à* l'**importance** (la «légitimité», pour reprendre la terminologie de la jurisprudence) de l'objectif atteint **dans le contexte donné**.

Un examen en bonne et due forme, à la fois exhaustif et exact, suppose que les différents éléments sur lesquels la mise en balance repose soient expressément déterminés et structurés dans un cadre cohérent.

Il est donc primordial que la mesure limitant les droits fondamentaux à la vie privée et/ou à la protection des données soit **suffisamment claire** pour que l'importance de l'ingérence puisse être déterminée. Celle-ci est en retour nécessaire pour vérifier si l'incidence de la mesure sur ces droits fondamentaux est bien «proportionnelle au but visé» (c'est-à-dire à l'objectif poursuivi par la législation qui fait l'objet du contrôle).

Comme l'a rappelé la CJUE, il est essentiel de souligner que la proportionnalité doit faire l'objet d'une évaluation ***in concreto***, au cas par cas:

> *«En application du principe de **proportionnalité**, il incombe à la juridiction de renvoi de prendre en considération **toutes les circonstances de l'affaire dont elle est saisie**, notamment la durée de la violation des règles mettant en œuvre la directive 95/46 ainsi que l'importance, pour les intéressés, de la protection des données divulguées»*[28] (caractères gras ajoutés).

---

[25] Voir la page 9 de l'avis 01/2014 du groupe de travail «article 29» sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, 27 février 2014, disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_fr.pdf.

[26] Lee A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, 2014, page 147.

[27] Conseil de l'Europe, **convention modernisée pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel,** texte consolidé, disponible à l'adresse suivante: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65c0.

[28] CJUE, affaire C-101/01, *Linqvist*, ECLI:EU:C:2003:596, point 89.

En d'autres termes, l'analyse de la proportionnalité est toujours **liée au contexte**[29]: comme il est expliqué plus loin dans les présentes lignes directrices, cette analyse ne peut être effectuée sans que le contexte de la mesure examinée n'ait été préalablement défini (par exemple, *le responsable du traitement partage-t-il ou octroie-t-il l'accès aux informations relatives à l'intéressé? avec qui et à quelle fin?*).

> La partie opérationnelle des présentes lignes directrices fournit des orientations à cet égard. À l'instar de la méthodologie d'analyse d'impact établie par la Commission, les lignes directrices relatives au principe de proportionnalité visent, en substance, à **aider le législateur à se poser les bonnes questions** au regard des aspects les plus pertinents et les plus récurrents de la protection des données. Dans les présentes lignes directrices, la liste des points à vérifier qui suit (un outil analytique en quatre étapes) vise également à stimuler une réflexion hors des sentiers battus, génératrice de choix politiques innovants *ex ante*, et à faciliter le contrôle et l'évaluation des mesures a posteriori.

III. Liste des points à vérifier pour évaluer la proportionnalité de toute nouvelle mesure législative

1. Description générale de la séquence des opérations

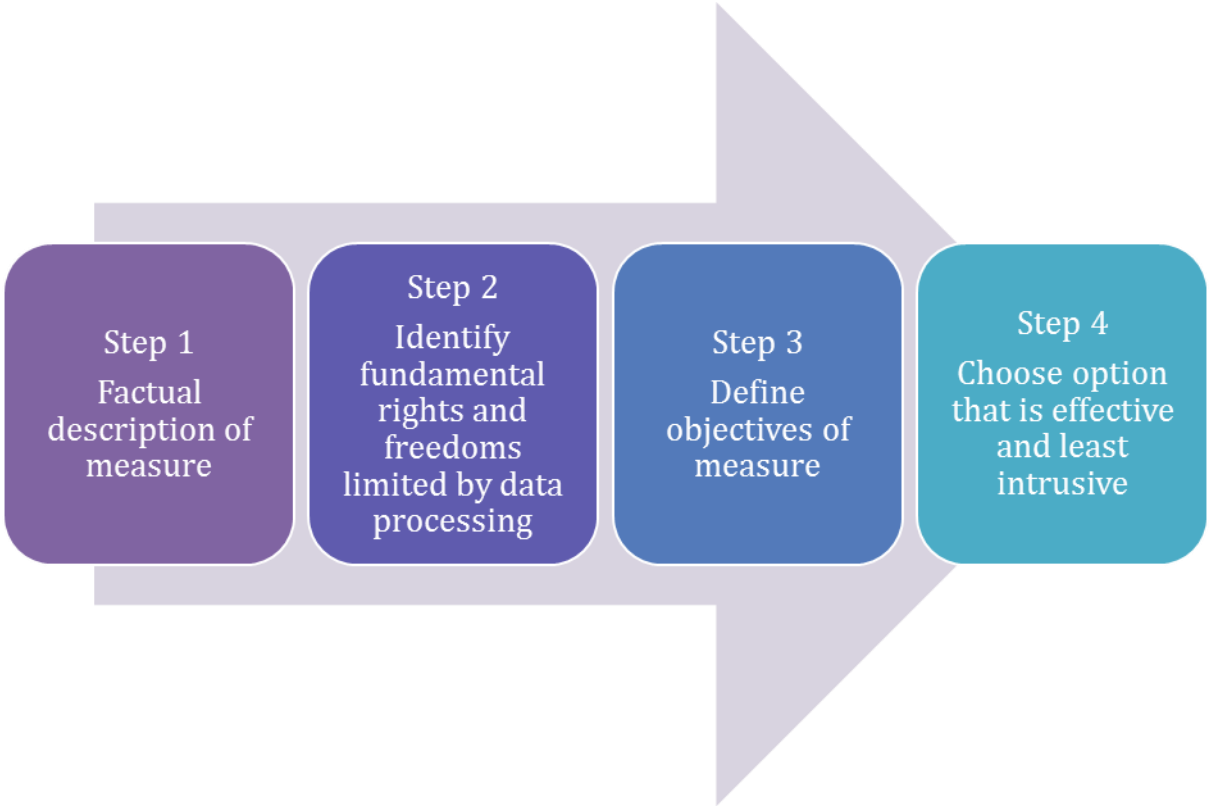
L'évaluation d'ensemble des critères de nécessité et de proportionnalité (**vue synoptique**) se présente comme suit:

Premier critère: Pour l'évaluation du critère de la nécessité, les étapes suivantes sont recommandées dans le guide pour l'évaluation de la nécessité[30]:

- L'**étape 1** est préliminaire; elle exige **une description factuelle détaillée** de la mesure proposée et de son objectif, préalablement à toute évaluation.
- L'**étape 2** permet de déterminer si la mesure proposée constitue **une limitation** des droits à la protection des données à caractère personnel ou au respect de la vie privée (également appelé «droit à la vie privée»), mais aussi, le cas échéant, d'autres droits.
- L'**étape 3** tient compte de l'**objectif de la mesure** pour évaluer la nécessité de celle-ci.
- L'**étape 4** fournit des **indications sur les aspects spécifiques à prendre en considération** lors du contrôle de la satisfaction du critère de la nécessité, la mesure devant, en particulier, être **efficace** et **la moins intrusive** possible.

[29] À titre d'exemple, voir l'arrêt de la Cour EDH, *M.K. c. France,* point 46: «[L]a Cour estime que l'État défendeur a **outrepassé sa marge d'appréciation en la matière**, le régime de conservation dans le fichier litigieux des empreintes digitales de personnes soupçonnées d'avoir commis des infractions mais non condamnées, **tel qu'il a été appliqué au requérant en l'espèce**, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une **atteinte disproportionnée** au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique» (caractères gras ajoutés).

[30] Voir page 9 du guide pour l'évaluation de la nécessité du CEPD.



Step	Étape
Factual description of measure	Description factuelle de la mesure
Identify fundamental rights and freedoms limited by data processing	Détermination des libertés et des droits fondamentaux limités par le traitement des données
Define objectives of measure	Définition des objectifs de la mesure
Choose option that is effective and least intrusive	Choix de l'option efficace et la moins intrusive

Si l'évaluation de la mesure conduit à la conclusion qu'une mesure satisfait à l'exigence de nécessité (**premier critère**), alors la mesure peut être examinée en suivant les étapes de l'évaluation du principe de proportionnalité (**second critère**) détaillées ci-dessous.

En d'autres termes, dans le cadre du **second critère**, nous examinerons à nouveau la mesure jugée nécessaire (soit la moins intrusive des mesures efficaces existantes permettant d'atteindre l'objectif poursuivi) pour déterminer si la limitation (l'ingérence) qu'elle engendre est proportionnelle à l'objectif recherché.

Deuxième critère: Pour l'évaluation du critère de proportionnalité, les étapes sont les suivantes:

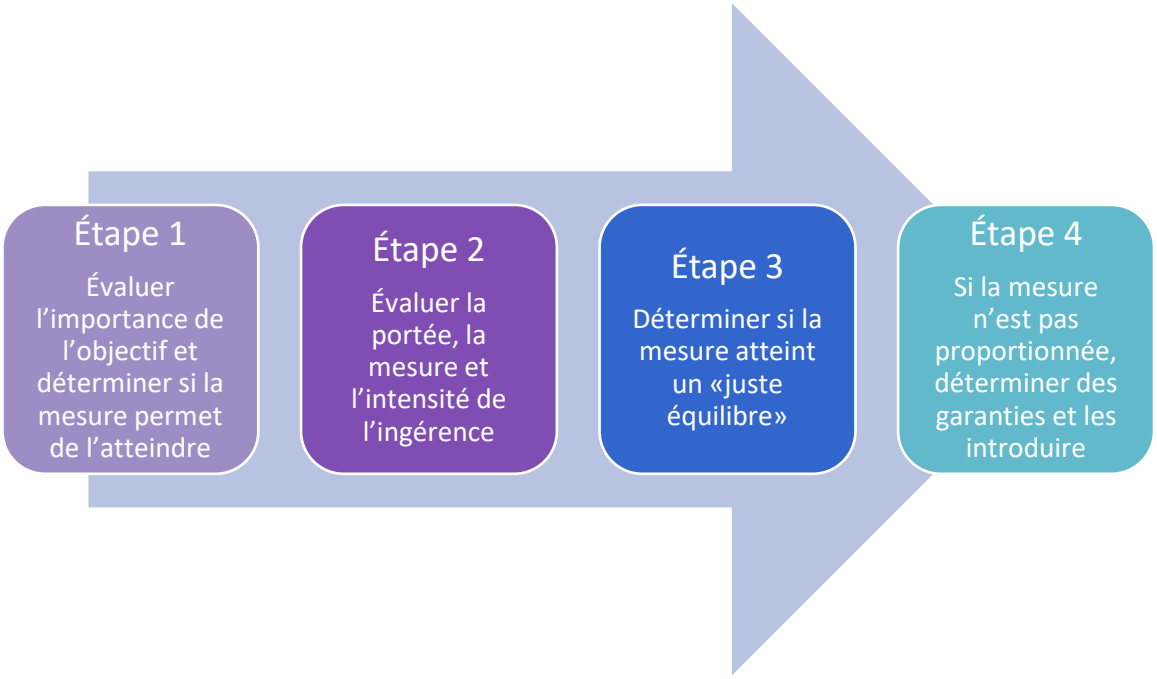
- **Étape 1** (ou étape 5 de la séquence globale des opérations): évaluer **l'importance** («**la légitimité**») **de l'objectif** (précisé à l'étape 3 du guide pour l'évaluation de la nécessité) et **déterminer si, et dans quelle mesure**, la proposition de mesure permet d'atteindre

cet objectif et répond au problème relevé dans la phase de définition du problème («**répond effectivement**») [soit «l'avantage/le bénéfice»].

- **Étape 2** (ou 6 de la séquence globale des opérations): évaluer **la portée, la mesure et l'intensité** de l'ingérence (déterminée à l'étape 2 du guide pour l'évaluation de la nécessité) en termes d'**incidence** sur les droits fondamentaux à la vie privée et à la protection des données [soit «l'inconvénient/le coût»].

- **Étape 3** (ou 7 de la séquence globale des opérations): déterminer si la mesure atteint un **juste équilibre (*avantages/inconvénients*; *bénéfices/coûts*)**.

- **Étape 4** (ou 8 de la séquence globale des opérations): **se prononcer sur la mesure («validation/non validation»)**. Si la proposition de mesure n'est pas validée, déterminer et introduire des garanties (si elles existent) pour rendre la mesure proportionnée, en tenant compte de tous les facteurs ayant permis de déterminer que la mesure était disproportionnée.



Step	Étape
Assess the importance of the objective and whether the measure meets the objective	Évaluer l'importance de l'objectif et déterminer si la mesure permet de l'atteindre
Assess the scope, the extend and the intensity of the interference	Évaluer la portée, la mesure et l'intensité de l'ingérence
Proceed to the 'fair balance' evaluation of the measure	Déterminer si la mesure atteint un «juste équilibre»
If the measure is not proportionate, identify and introduce safeguards	Si la mesure n'est pas proportionnée, déterminer des garanties et les introduire

2. Description des étapes de l'évaluation du critère de proportionnalité

Étape 1: évaluer l'importance (la légitimité) de l'objectif et déterminer si et dans quelle mesure la mesure proposée permet d'atteindre cet objectif (efficacité)

Une description détaillée du ou des **objectif**(s) de la mesure envisagée n'est pas uniquement une **condition préalable** à l'évaluation de la nécessité. Elle permet également de démontrer que la mesure satisfait à la première condition énoncée à l'article 52, paragraphe 1, de la charte, à savoir qu'elle doit être *prévue par la loi*[31].

En pratique, si la législation ne **définit pas clairement et de manière spécifique l'objectif** ou les objectifs en jeu, il est impossible de procéder à une évaluation *ex ante* de l'importance de l'objectif et de la capacité de la mesure à atteindre celui-ci.

Il est important ici de rappeler que, à ce stade, tant la **mesure** que ses **objectifs** devraient déjà avoir été **définis** aux étapes 1 et 3 de l'évaluation du critère de la nécessité (premier critère). Cette étape consiste à examiner de nouveau ces objectifs en vue de vérifier, toujours *ex ante* mais, maintenant, *in concreto*, leur **importance**, et dans quelle mesure la mesure permettra de les **réaliser efficacement**.

> En ce qui concerne la terminologie utilisée dans le cadre de l'analyse d'impact de la Commission, il est ici question de l'efficacité (*la mesure proposée est-elle la plus à même d'atteindre les objectifs?*) et de l'efficience (*le rapport coût/efficacité*) de la mesure (l'option stratégique définie) à atteindre l'objectif (c'est-à-dire à **résoudre les problèmes relevés à l'étape de la définition du problème**).

La mesure doit répondre aux **besoins** (c'est-à-dire les objectifs d'intérêt général reconnus par l'Union européenne ou le besoin de protéger les droits et les libertés d'autrui) **clairement définis lors de l'étape de l'analyse du problème**. Comme l'a rappelé la CJUE, la **mesure**,

---

[31] Tel que l'avocat général Mengozzi l'exprime dans ses conclusions relatives au projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens (ECLI:EU:C:2016:656, point 193): «*Selon la jurisprudence de la Cour EDH, cette expression exige, en substance, que la mesure en cause soit* ***accessible*** *et* ***suffisamment prévisible****, soit, autrement dit, qu'elle use des termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la CEDH*» (caractères gras ajoutés).
- Dans les conclusions rendues dans les affaires jointes C-203/15 et C-698/15 (*Tele2 Sverige AB*, ECLI:EU:C:2016:572, points 139 et 140), l'avocat général Saugmandsgaard Øe détaille plus avant: «*Selon cette jurisprudence, l'expression "prévue par la loi" implique que la base légale soit suffisamment accessible et prévisible, c'est-à-dire* ***énoncée avec assez de précision pour permettre à l'individu, en s'entourant au besoin de conseils éclairés, de régler sa conduite****. Cette base légale doit également fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes (principe de la prééminence du droit). Or, il est selon moi nécessaire que l'expression 'prévue par la loi' utilisée à l'article 52, paragraphe 1, de la [c]harte se voie attribuer une portée similaire à celle que revêt cette expression dans le contexte de la CEDH*».
À cet égard, voir également l'arrêt de la Cour EDH, *Catt c. Royaume-Uni*, 24 janvier 2019, point 6 des conclusions concordantes de la juge Koskelo et du juge Felici: «**les principes généraux du droit de la protection des données**, tels que l'exigence que les données traitées soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard de cette finalité, **se trouvent affaiblis, jusqu'à en devenir potentiellement inopérants, lorsque l'objectif lui-même est dénué de toute définition ou de limitation pertinente**.» (caractères gras ajoutés).

pour être proportionnée, doit «répondre effectivement» à l'**objectif**[32]. L'objectif doit également refléter les besoins relevés lors de l'analyse du problème.

Lors de l'évaluation de l'efficacité de la mesure, le législateur doit toujours vérifier en premier lieu l'efficacité des **mesures déjà existantes**[33]. En d'autres termes, avant de proposer ou d'adopter de nouvelles mesures, le législateur doit déterminer si les «mesures existantes» sont réellement **appliquées**, et si **l'élargissement et/ou l'approfondissement** de ces mesures seraient déjà susceptibles de répondre de manière satisfaisante au problème relevé à l'étape de l'analyse du problème. À défaut d'une évaluation systématique de l'efficacité des mesures existantes poursuivant un objectif similaire ou identique, il sera considéré que l'examen du critère de la proportionnalité d'une nouvelle mesure n'a pas été réalisé en bonne et due forme. S'il existe déjà une mesure, il conviendra, au cours de la mise en balance, de considérer l'efficacité non de manière absolue mais par rapport à la **valeur ajoutée** qu'apporte la nouvelle mesure.

Procédure à suivre

- Les **besoins** doivent faire l'objet d'une description suffisamment détaillée au stade de l'analyse du problème pour que la *raison* pour laquelle l'initiative a été engagée soit clairement comprise. Le législateur doit détenir des informations exhaustives et exactes sur les**problèmes à résoudre** (les **facteurs** du problème) ainsi que sur les options disponibles.

---

[32] Arrêt de la CJUE du 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, Tele2 Sverige, ECLI:EU:C:2016:970, point 94: «*Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à l'exercice de ces droits et de ces libertés que si elles sont nécessaires et* ***répondent effectivement*** *à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui*» (caractères gras ajoutés).

[33] Dans son avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif (disponible à l'adresse https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_fr.pdf), le groupe de travail «article 29» affirme ce qui suit: «Quelle que soit la façon dont cette appréciation est effectuée, elle doit comporter une explication, étayée par des éléments de preuve, des raisons pour lesquelles les mesures existantes ne suffisent plus à répondre au besoin.»

À la page 3 de son **avis 06/2016 sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne**, 21 septembre 2016 (disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_fr.pdf), le CEPD fait observer que «la nécessité et la proportionnalité de l'EES [le système d'entrée/de sortie] doivent être appréciées aussi bien de manière globale, **compte tenu des systèmes informatiques à grande échelle qui existent déjà au sein de l'UE**, que de manière spécifique, dans le cas particulier des ressortissants de pays tiers qui se rendent légalement dans l'UE».

- À la page 8 de son **avis 3/2017 sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)**, 6 mars 2017 (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-03-070_etias_opinion_fr.pdf), le CEPD affirme sans ambiguïté ce qui suit: «[Une] analyse d'impact de l'ETIAS sur le respect de la vie privée et la protection des données doit **prendre en considération toutes les mesures adoptées à l'échelle de l'Union européenne concernant les objectifs en matière de migration et de sécurité et analyser en profondeur leur application concrète, leur efficacité et leur incidence sur les droits fondamentaux des personnes avant que de nouveaux systèmes entraînant le traitement de données à caractère personnel ne soient créés**. Cette analyse doit tenir compte des domaines d'action dans lesquels les mesures s'appliquent et du rôle respectif de chacun des acteurs clés concernés.»

- Voir la page 15 de **l'avis 5/2015 du CEPD sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière**: «La proposition ne prévoit pas d'évaluation exhaustive de la capacité des instruments existants actuels à atteindre la finalité du système PNR de l'UE.»

- Notamment, pour ce qui est du problème à résoudre (**définition du problème**), le législateur doit être conscient du **degré d'urgence pour l'intérêt public** (par exemple, la sécurité publique) à prendre en considération, et **y faire clairement référence** dans la mesure (en indiquant, par exemple, que la mesure est destinée à répondre à un niveau temporairement élevé de menace). On peut résumer cette démarche par la question suivante: «Existe-t-il un *besoin social impérieux* de limiter le droit (à la vie privée et/ou à la protection des données)?»[34].

- En se référant au **niveau de menace** évoqué ci-dessus, et en assurant le contrôle/suivi de ce facteur, le législateur doit pouvoir suspendre la mesure limitant les droits à la vie privée et à la protection des données à caractère personnel une fois que ce niveau diminue. Un système de contrôle indépendant est également essentiel pour éviter que des mesures temporaires ne deviennent permanentes.

- Il est important de vérifier que la ou les **finalités concrètes** de la mesure **reflètent** bien ces besoins. On peut résumer cette démarche par la question suivante: «La mesure envisagée correspond-elle à ce besoin?» [pour reprendre la terminologie de l'analyse d'impact, «*Si l'on prend en considération son incidence/ses conséquences, la mesure résout-elle le problème?*»] Répondre à cette question par l'affirmative permet d'éviter un «détournement de la fonction législative» (c'est-à-dire une mesure qui ne résout pas effectivement le problème[35] mais correspond en réalité à une finalité différente).

---

[34]Voir, par exemple, l'arrêt de la Cour EDH dans l'affaire *Saravia c. Allemagne*, point 112: «Ces vastes pouvoirs de surveillance **n'auraient pas répondu à un besoin impérieux** de la société en la matière. La République fédérale d'Allemagne n'aurait pas été sous la menace d'une attaque armée d'un État étranger possédant l'arme nucléaire, comme elle l'aurait été durant la "Guerre froide". Il n'y aurait eu aucun autre danger comparable à conjurer. En particulier, le trafic de stupéfiants, le faux-monnayage et le blanchiment d'argent ou d'autres risques présumés relevant du crime organisé n'auraient pas suffisamment menacé la sûreté publique pour justifier une ingérence aussi importante dans les télécommunications d'individus. La limitation des interceptions aux informations "pertinentes" ("*nachrichtendienstliche Relevanz*") pour le service des renseignements ordonnée par la Cour constitutionnelle fédérale dans son arrêt n'aurait pas suffi à restreindre effectivement les pouvoirs de surveillance du service fédéral des renseignements» (caractères gras ajoutés).
Au sujet de la notion de besoin social impérieux, voir les précisions fournies aux pages 7 et 8 de l'avis du **groupe de travail «article 29» sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif**, WP211, 27 février 2014. Voir également la liste de facteurs à prendre en considération, aux pages 9 à 11. L'avis est disponible à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp211_fr.pdf.

[35] Voir le **document de synthèse sur l'interopérabilité des systèmes d'information au sein de l'espace de liberté, de sécurité et de justice**, 17 novembre 2017 (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_fr_0.pdf), dans lequel le CEPD observe que la Commission «devra également établir clairement quelles catégories de données à caractère personnel seraient traitées, et **à quelles fins spécifiques**, dans le contexte de ses futures initiatives en matière d'interopérabilité. Cela permettra d'engager un vrai débat sur l'interopérabilité sous l'angle des droits fondamentaux.» (page 3).
Dans la même ordre d'idée, voir l'**avis 4/2018 du CEPD sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE**, 16 avril 2018, disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-04-16_edps-opinion-on-interoperability_fr.pdf.
«41. Le CEPD met l'accent sur le fait que la formulation "combattre la migration irrégulière et favoriser un niveau élevé de sécurité" est une description très générale des finalités (par ailleurs légitimes). Il relève que l'article 20 prévoit l'adoption de mesures législatives nationales censées préciser ces finalités. Il tient néanmoins à rappeler que la Cour de justice de l'Union européenne ("CJUE"), dans son arrêt Digital Rights Ireland (point 61), a considéré que

- Vérifier que la **finalité (**l'**objectif)** inscrite dans la proposition de législation correspond à **l'impératif réglementaire public/sociétal** auquel elle prévoit de répondre (le préjudice auquel la société pourrait être exposée en l'absence de la mesure, par exemple une augmentation de la délinquance ordinaire ou certains crimes en col blanc).

> Nous rappelons qu'en matière d'analyses d'impact de la Commission, les **objectifs**doivent être **SMART**, c'est-à-dire: **spécifiques** (suffisamment précis et concrets); **mesurables** (définir un état souhaité dans l'avenir en termes quantifiables, par exemple une baisse de la criminalité estimée à .. %); **réalisables** («achievable»); **réalistes**; et **délimités dans le temps** («time-dependent»: associés à une date ou à une période fixe à laquelle les résultats devraient être obtenus). Ces exigences, communes à l'ensemble de la méthodologie pour une meilleure réglementation, sont particulièrement importantes, comme le montreront les exemples, dans le cas de législations limitant ou ayant tout autre incidence sur la protection des données à caractère personnel.

- Évaluer **l'importance** de l'objectif (s'agit-il de protéger une valeur constitutionnelle ou un droit fondamental?[36]).

- Évaluer **l'efficacité et l'efficience** de la mesure à répondre à cet objectif.

Exemples pertinents

Nous illustrerons notamment cette **méthodologie** par **l'analyse détaillée**, dans les quatre encadrés sur fond gris proposant des exemples pour chacune des quatre étapes, des arrêts de la CJUE dans les affaires *Tele2* et *Ministerio Fiscal*, des conclusions de l'avocat général et de l'avis 1/15 de la CJUE dans l'affaire «Accord entre le Canada et l'Union européenne sur le

---

la directive 2006/24 "*ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions*", se bornant à renvoyer "*de manière générale aux infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne."* La Cour a également considéré que l'accès et l'utilisation des données n'étaient pas "s*trictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci*".

42. **Le CEPD considère que les finalités consistant à combattre la migration irrégulière et favoriser un niveau élevé de sécurité, dans le cadre de l'article 20, sont trop générales et ne répondent pas aux exigences de finalités "*strictement restreintes*" et "*précisément délimitées*" dans les propositions, comme l'exige la Cour. Il recommande donc de les définir plus précisément dans les propositions**. Ainsi, par exemple, "migration irrégulière" pourrait renvoyer aux conditions d'entrée et de séjour telles qu'elles sont visées à l'article 6 du règlement (UE) 2016/399 du Parlement européen et du Conseil du 9 mars 2016 concernant un code de l'Union relatif au régime de franchissement des frontières par les personnes. En ce qui concerne la sécurité, le CEPD recommande de cibler les infractions pénales qui sont susceptibles, en particulier, de menacer un niveau élevé de sécurité, par exemple en renvoyant aux infractions pénales énumérées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI si elles sont passibles, en vertu du droit national, d'une peine ou d'une mesure de sûreté privatives de liberté pour une période maximale d'au moins trois ans.».

[36] Pour un **aperçu des droits, des libertés et des principes garantis par la charte**, voir l'annexe II, page 28, du document de travail des services de la Commission, «Orientations opérationnelles sur la prise en compte des droits fondamentaux dans les analyses d'impact de la Commission», SEC(2011) 567 final.

transfert des données des passagers aériens», ainsi que de l'arrêt de la CJUE dans l'affaire *Bevándorlási és Állampolgársági Hivatal*.

EXEMPLE 1: Tele2 Sverige AB (CJUE, C-203/15, ECLI:EU:C:2016:970)

La Cour **décrit ainsi les objectifs** de la mesure examinée (pour résumer, une obligation concernant la conservation de données relatives au trafic et de données de localisation): «*l'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les mesures législatives qu'il vise et qui dérogent au principe de confidentialité des communications et des données relatives au trafic y afférentes doivent avoir pour* ***objectif*** *de "****sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou [d']assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques****", ou doivent poursuivre un des autres objectifs visés à* ***l'article 13, paragraphe 1****, de la directive 95/46, auquel renvoie l'article 15, paragraphe 1, première phrase, de la directive 2002/58 [...]. Une telle* ***énumération d'objectifs revêt un caractère exhaustif*** *ainsi qu'il ressort de l'article 15, paragraphe 1, deuxième phrase, de cette dernière directive, aux termes duquel les mesures législatives doivent être justifiées par "un des motifs énoncés" à l'article 15, paragraphe 1, première phrase, de ladite directive. Partant, les États membres* ***ne sauraient adopter de telles mesures à d'autres fins que celles*** *énumérées à cette dernière disposition*» (caractères gras ajoutés). Bien que **l'importance** de l'objectif (la protection de la sécurité du public et l'application du droit pénal) ne fasse aucun doute, la Cour a en outre reconnu que la mesure améliorerait les possibilités d'utilisation des techniques modernes d'enquête, et, par conséquent, «*l'****efficacité*** *de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme*» (caractères gras ajoutés).

EXEMPLE 2: Ministerio Fiscal (CJUE, C-207/16, ECLI:EU:C:2018:788)

En ce qui concerne **l'importance de l'objectif**, la Cour reconnaît que **l'objectif** de la mesure est limité à la ***«prévention, de recherche, de détection et de poursuite d'infractions pénales en général»*** (en l'espèce, le vol d'un portefeuille et d'un téléphone portable) par opposition à «la criminalité grave». Dès lors, on peut affirmer que la Cour considère que le «degré» d'importance de l'objectif est relativement **faible**.

À propos de l'**efficacité de la mesure** à atteindre l'objectif précité, la Cour fait remarquer qu'au moyen de la mesure examinée « *la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'****accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques****, [...]* ***[à] identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé****». «* *les données visées par la demande d'accès en cause au principal* ***permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM****» (caractères gras ajoutés). Il est, partant, incontestable que la mesure serait* ***efficace*** *aux fins de retrouver la trace, s'il y en a, du voleur ou de l'acquéreur du téléphone (au cas où celui-ci déciderait d'utiliser le téléphone en y installant une carte SIM), et d'aider à identifier, directement ou indirectement, au moyen des recherches supplémentaires ainsi facilitées, l'auteur de l'infraction*.

EXEMPLE 3: «Accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens» (conclusions de l'avocat général, ECLI:EU:C:2016:656, et avis 1/15 de la CJUE, ECLI:EU:C:2017:592)

L'avocat général Mengozzi, au point 205 de ses conclusions, reconnaît tant **l'importance de l'objectif** que **l'efficacité** de la mesure à atteindre cet objectif: «*je ne pense pas qu'il existe de véritables obstacles à reconnaître que l'ingérence que comporte l'accord envisagé* ***soit apte à réaliser l'objectif de sécurité publique****, en particulier de lutte contre le terrorisme et la criminalité transnationale grave, poursuivi par ce dernier. En effet, ainsi que l'ont fait notamment valoir le gouvernement du Royaume-Uni et la Commission, la transmission de données PNR en vue de leur analyse et de leur conservation permet aux autorités canadiennes de disposer de possibilités supplémentaires d'identification de passagers,*

*jusque-là inconnus et non soupçonnés, qui pourraient présenter des liens avec d'autres personnes et/ou passagers impliqués dans un réseau terroriste ou participant à des activités de criminalité transnationale grave. Ces données, **ainsi que l'illustrent les statistiques** communiquées par le gouvernement du Royaume-Uni et la Commission à propos de la pratique passée des autorités canadiennes, constituent **des instruments utiles pour les enquêtes pénales**, qui sont également de nature à favoriser, au regard notamment de la coopération policière instituée par l'accord envisagé, la prévention et la détection d'une infraction terroriste ou d'un acte de criminalité transnationale grave à l'intérieur de l'Union*» (caractères gras ajoutés).

Tenant compte des **mesures déjà existantes**, la Cour conclut que les données déjà disponibles «*ne seraient donc **pas suffisantes** pour réaliser avec une efficacité comparable l'objectif de sécurité publique poursuivi par l'accord envisagé*» (caractères gras ajoutés).

EXEMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJUE, C-473/16, ECLI:EU:C:2018:36)

Dans cette affaire, la mesure examinée prévoit la collecte et le traitement du **rapport d'un psychologue** portant sur l'orientation sexuelle d'une personne ayant sollicité le statut de réfugié au titre de la directive 2011/95 du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, à un statut uniforme pour les réfugiés ou les personnes pouvant bénéficier de la protection subsidiaire, et au contenu de cette protection (JO L 337, 20.12.2011, p. 9). La Cour relève que **l'objectif** de la mesure est «*la recherche d'éléments permettant d'apprécier ses besoins réels de protection internationale*».

La Cour observe également que «***le caractère approprié** d'une expertise telle que celle en cause au principal ne pourra être admis que si celle-ci est fondée sur des méthodes et des principes suffisamment fiables au regard des normes admises par la communauté scientifique internationale*» (caractères gras ajoutés).

Pourtant, au regard de **l'efficacité** de la mesure à atteindre l'objectif mentionné, la Cour relève que: «*une telle expertise **ne saurait être regardée comme étant indispensable** en vue de confirmer les déclarations d'un demandeur de protection internationale relatives à son orientation sexuelle afin de se prononcer sur une demande de protection internationale motivée par une crainte de persécution en raison de cette orientation*» (caractères gras ajoutés).

Elle juge en particulier que: «*lorsque les États membres appliquent le principe selon lequel il appartient au demandeur d'étayer sa demande, les déclarations du demandeur relatives à son orientation sexuelle qui ne sont pas étayées par des preuves documentaires ou d'une autre nature **ne nécessitent pas confirmation lorsque les conditions énoncées à cette disposition sont remplies, sachant que ces conditions renvoient notamment à la cohérence et à la plausibilité de ces déclarations** et **ne se réfèrent en aucune manière à la réalisation ou à l'utilisation d'une expertise***» (caractères gras ajoutés).

«*Par ailleurs, à supposer même qu'une expertise fondée sur des tests projectifs de la personnalité, telle que celle en cause au principal, **puisse contribuer** à déterminer avec une certaine fiabilité l'orientation sexuelle de la personne concernée, il ressort des énonciations de la juridiction de renvoi que **les conclusions d'une telle expertise seraient seulement susceptibles de donner une image** de cette orientation sexuelle. Partant, ces conclusions présentent, en tout état de cause, un **caractère approximatif et n'ont donc qu'un intérêt limité** pour apprécier les déclarations d'un demandeur de protection internationale, en particulier lorsque, comme dans l'affaire en cause au principal, ces déclarations sont dénuées de contradiction*» (caractères gras ajoutés).

EXEMPLE 5: Avis du CEPD 3/2017 sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

Il arrive que le législateur définisse également **l'objectif** de la mesure comme «**un risque à éviter**». Dans cette affaire également, comme le souligne le CEPD, les risques doivent être définis aussi précisément que possible. «L'article premier de la proposition établit que la finalité de l'ETIAS est de

déterminer si la présence de voyageurs exemptés de l'obligation de visa sur le territoire des États membres pose un **risque en matière d'immigration irrégulière, de sécurité et/ou de santé publique**. Le CEPD relève que la proposition **définit le risque en matière de santé publique** sur la base de catégories spécifiques de maladies mais **n'offre aucune définition des risques en matière de sécurité ou d'immigration irrégulière**» (caractères gras ajoutés).

Étape 2: évaluer (la portée, la mesure, et l'intensité de) l'ingérence, soit l'incidence réelle de la mesure sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel

L'évaluation détaillée de l'ingérence de la mesure envisagée dans les droits fondamentaux à la vie privée et à la protection des données à caractère personnel constitue une autre étape essentielle de l'examen du critère de la proportionnalité.

Il est important de rappeler que **les libertés et les droits fondamentaux limités** par la mesure ont déjà été **définis** à l'étape 2 de l'évaluation du critère de la nécessité (premier critère). À cette étape, nous réexaminerons ces droits fondamentaux et ces libertés fondamentales aux fins de déterminer, toujours *ex ante*, mais *in concreto*, la manière dont ils seraient affectés. En effet, comme mentionné dans le manuel de la FRA «Application de la Charte des droits fondamentaux de l'Union européenne dans le processus législatif et l'élaboration des politiques à l'échelle nationale - Orientations», «*la mesure ne doit pas faire porter une* ***charge disproportionnée et excessive*** *sur les personnes concernées par la limitation par rapport à l'objectif recherché*»[37].

Il est important de signaler que l'incidence peut être **faible** pour **l'individu** concerné, mais n'en être pas moins **considérable ou très considérable** à titre collectif, **pour la société** dans son ensemble (**incidence sur les individus** *par rapport à* **incidence sur la société dans son ensemble**)[38].

Le **coût** de la mesure affectant la vie privée, vus sous cet angle, est représenté par les **externalités**, les effets externes de l'absence de protection des données (la «pollution des données»). Parmi les exemples hypothétiques de tels effets externes figurent le préjudice pour le processus électoral et politique (usage abusif des données à des fins de manipulation politique)[39], le profilage illégal et la discrimination engendrant une défiance à l'égard des

[37] Manuel de la FRA cité ci-dessus, page 76. Voir également l'arrêt de la CJUE dans l'affaire C-258/14, *Eugenia Florescu e.a./Casa Judeţeană de Pensii Sibiu e.a.*, ECLI:EU:C:2017:448, point 58.

[38] Voir Omri Ben-Shahar, *Data Pollution*, University of Chicago, Juin 2018, disponible à l'adresse: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191231 page 3: «Le paradigme de la vie privée est fondé sur l'hypothèse que le dommage causé par les entreprises consacrées aux données personnelles est par nature privé - il blesse le "moi profond ". Pourtant, par un simple effet d'accumulation (ou par des moyens plus nuancés), ces blessures profondément privées ont un impact social par dérivation»; et page 4: «Une littérature pléthorique a examiné tous les aspects possibles des dommages privés causés par la collecte de données, les éventuelles blessures à la vie privée que subissent les individus dont les données sont collectées. Le **problème de l'externalité**, toutefois, a été complétement négligé: de quelle manière la participation des individus aux services de récolte de données affecte **autrui, ainsi que l'ensemble du public**.»

[39] Voir l'avis du CEPD sur la manipulation en ligne auquel il est fait référence dans la note 42 ci-dessous.
ICO, "*Democracy disrupted? Personal information and political influence*", 11 juillet 2018, disponible à l'adresse: https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf.
Communication conjointe au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions: *Plan d'action contre la désinformation*, (JOIN(2018) 36 final) disponible à l'adresse:

autorités publiques, l'«effet dissuasif» de mesures de surveillance générale sur la liberté d'expression[40], ou d'autres effets négatifs sur la liberté des individus engendrés par la mise en œuvre de systèmes de profilage et de notation[41].

Bien qu'elles soient difficiles à quantifier en pratique[42], ces externalités doivent être prises en considération par le législateur lors de son évaluation du «coût pour la vie privée» de la mesure.

S'il s'agit d'une proposition de mesure de surveillance, il est important de déterminer le **degré d'intrusion** que suppose la méthode de surveillance envisagée. Dans le cadre de cette évaluation, il convient d'examiner les **dimensions de la surveillance**. La jurisprudence pertinente de la Cour EDH et de la CJUE a déterminé les différentes dimensions de la surveillance, depuis les «dimensions liées aux sens» (telles que les enregistrements audio et vidéo)[43] jusqu'aux possibilités en matière d'analyse, de fusion et de communication des informations. Le **degré d'intrusion** dans la vie privée des individus ciblés, ainsi que l'intrusion potentielle dans la vie privée de **tiers**, doivent être soigneusement évalués par les autorités qui se prononceront sur la mesure.

Lors de cette étape, l'incidence se mesure également aux **effets préjudiciables** potentiels de la mesure **au-delà du point de vue de la protection de la vie privée** et doit donc inclure les risques existant pour d'autres droits fondamentaux. Cette approche est conforme à celle adoptée dans le RGPD, lequel fait référence, explicitement et à de nombreuses reprises, aux «risques pour les droits et les libertés des personnes physiques», soulignant ainsi le fait que tout effet préjudiciable pour le droit à la vie privée est souvent, de fait, **également**

---

https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Garantir des élections européennes libres et équitables», disponible à l'adresse: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-free-fair-elections-communication-637_en.pdf.

[40] Dans ses conclusions relatives à l'affaire *Digital Rights* (ECLI:EU:C:2013:845), l'avocat général Cruz Villalón fait référence à cet effet dissuasif: «*[I]l ne saurait, certes, être négligé que le sentiment diffus de surveillance que la mise en œuvre de la directive 2006/24 peut engendrer est susceptible d'exercer une influence décisive sur l'exercice par les citoyens européens de leur liberté d'expression et d'information et que l'existence d'une ingérence dans le droit garanti par l'article 11 de la [c]harte doive, par conséquent, également être constatée*» (point 52); «*La collecte de ces données crée les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée. Le sentiment diffus de surveillance généré pose de manière particulièrement aiguë la question de la durée de conservation des données*» (point 72).
La CJUE a confirmé l'approche de l'avocat général en estimant, au point 37 de l'arrêt, que «*[...] la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante*».

[41] Voir, pour des exemples hypothétiques, H.J. Pandit, D. Lewis, *Ease and Ethics of User Profiling in Black Mirror*, 2018, disponible à l'adresse: https://dl.acm.org/citation.cfm?id=3191614. Pour un modèle d'analyse d'impact, voir «The Ethics Canvas", page 1582.

[42] Voir à la page 31 de «*Data Pollution*», cité à la note de bas de page 38: «En matière de données, les externalités sont souvent qualitatives et aléatoires. À quel montant peut-on chiffrer des élections présidentielles faussées? Le profilage racial discriminatoire?».

[43] Dans l'affaire *Uzun c. Allemagne*, la Cour EDH a estimé que l'utilisation d'un dispositif de localisation tel que le GPS constituait une mesure moins intrusive que l'interception de communications à caractère personnel.
- À propos de la **vidéosurveillance** (CCTV), voir les **lignes directrices du CEPD en matière de vidéosurveillance**, 17 mars 2010, disponibles à l'adresse: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_fr.pdf.

préjudiciable pour **d'autres droits fondamentaux** tels que les droits à **la liberté d'expression, à la libre circulation, à la liberté**

d'association[44], ainsi qu'aux principes généraux du droit de l'Union tels que le **principe de non-discrimination**[45]. En ce sens, les présentes lignes directrices adoptent une approche intégrant l'ensemble des droits fondamentaux.

Procédure à suivre

L'incidence doit être suffisamment décrite pour permettre de comprendre précisément **la portée, la mesure et le degré d'intrusion de l'ingérence** dans les droits fondamentaux à la vie privée et à la protection des données à caractère personnel. Il est essentiel, en particulier, de déterminer précisément:

- **l'incidence[46],** en prenant en considération:

[44] Le CEPD promeut une approche plus large de la protection des données qui prend en considération ces différentes facettes. Voir, en particulier, la page 13 de l'**avis 3/2018 du CEPD sur la manipulation en ligne et les données à caractère personnel**: «La vie privée et la protection des données à caractère personnel font partie des "libertés" de l'Union, qui comprennent **la liberté de pensée, de conscience et de religion**, **la liberté d'expression et d'information** et **la liberté de réunion et d'association** (articles 10, 11 et 12). Elles **sont également clairement en jeu** en raison de la capacité des grands intermédiaires de plateforme soit de faciliter soit d'entraver la diffusion de l'information. Par exemple, un contenu qui est mal indexé ou classé par un moteur de recherche en ligne est moins susceptible de toucher un grand public voire d'être vu. Autrement, un algorithme de recherche peut également présenter un biais vis-à-vis de certains types de contenu ou de fournisseurs de contenu, risquant ainsi d'affecter les valeurs afférentes telles que le pluralisme et la diversité des médias»; ainsi que page 5: «La législation de l'Union en matière de protection des données et de confidentialité des communications électroniques s'applique à la collecte de données, au profilage et au microciblage, et **si elle est correctement mise en œuvre, elle devrait contribuer à minimiser les préjudices** issus des tentatives de manipuler des personnes et des groupes.» L'avis est disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf.

[45] Par exemple, le Comité Meijers, dans ses «Commentaires sur la proposition de règlement du Parlement européen et du Conseil portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (coopération judiciaire et policière, asile et migrations), 12 décembre 2017, COM (2017) 794», 19 février 2018, a relevé l'intersection entre **la limitation de la vie privée** (collecte et traitement de données à caractère personnel relatives à un groupe ou une catégorie de personnes) **et la violation du principe de non-discrimination**. Voir page 3 des commentaires: "[L]'objectif explicite de la proposition visant à faciliter les contrôles d'identité de ressortissants de pays tiers par les organisations de police au sein du territoire de l'UE, à savoir vérifier si des informations sur l'individu sont conservées dans une ou plusieurs des bases de données de l'Union, augmentera la probabilité que les ressortissants de pays tiers (ou ceux qui seraient considérés comme tels) soient arrêtés aux fins de contrôler leur identité. Dans ce contexte, le comité Meijers rappelle l'affaire *Huber c. Allemagne*, dans laquelle la CJUE a examiné le **traitement différentié entre citoyens nationaux et citoyens de l'Union européenne** au regard de la **conservation dans un registre centralisé et de l'utilisation multiple de données à caractère personnel par une administration étrangère, notamment l'utilisation à des fins de répression** (CJUE, *Huber/Germany*, C-524/06, 16 décembre 2008, points 78 et 79).»

[46] L'analyse d'impact à laquelle ces lignes directrices font référence tient compte des **atteintes contextuelles à la protection des données et du risque d'atteinte pouvant résulter de la mesure législative faisant l'objet de l'évaluation, tant pour les individus que pour la société dans son ensemble**. Il s'agit donc d'une notion différente (plus large) de la notion de «**risques, dont le degré de probabilité et de gravité varie, pour les droits et les libertés des personnes physiques**» visée à l'article 24 du RGPD.
Ces lignes directrices diffèrent également de l'**analyse d'impact relative à la protection des données** (AIPD) au titre de l'article 35 du RGPD en ce qu'elles envisagent l'évaluation de la proportionnalité de la *mesure législative* à un niveau plus abstrait (et non comme s'il s'agissait d'un *type de traitement* envisagé par un responsable du traitement). Ainsi, l'évaluation du principe de proportionnalité peut être considérée comme une «*AIPD portant sur la loi*» (à réaliser dans le cadre de la fonction consultative du CEPD au regard des mesures législatives ayant une incidence sur le droit à la vie privée et à la protection des données à caractère personnel).

- *la **portée*** de la mesure: est-elle suffisamment délimitée? *nombre de personnes* concernées; risque éventuel d'«*intrusion **collatérale***», c'est-à-dire d'ingérence dans la vie privée de personnes autres que les personnes concernées par la mesure[47];

- *la **mesure***: *De quelle manière le droit est-il restreint? quantité d'informations* collectées; *durée de la collecte; besoin ou non, dans le cadre de la mesure examinée, de collecter et traiter des catégories particulières de données*[48];

Néanmoins, il n'est pas inutile de relever que **nombre des facteurs pertinents pour effectuer l'AIPD sont également pertinents dans le cadre de l'évaluation du coût d'une mesure législative en matière de vie privée.** À cet égard, voir les «**lignes directrices concernant l'analyse d'impact en matière de 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»**, WP248, telles que révisées en dernier lieu et adoptées le 4 octobre 2017, du groupe de travail «article 29» (désormais CEPD), et disponibles à l'adresse suivant: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.
Les neuf facteurs (caractérisant des risques élevés) suivants sont énumérés aux pages 9 à 11: (i) **Évaluation ou notation**, y compris les activités de profilage et de prédiction; (ii) **Prise de décisions automatisée** avec effet juridique ou effet similaire significatif; (iii) **Surveillance systématique**; (iv) **Données sensibles** ou données à caractère hautement personnel; (v) Données traitées **à grande échelle**; (vi) **Croisement ou combinaison** d'ensembles de données; (vii) **Données concernant des personnes vulnérables**; (viii) Utilisation innovante ou application de **nouvelles solutions technologiques ou organisationnelles**, utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, *etc*.; (ix) Traitements qui, en eux-mêmes, «**empêchent [les personnes concernées] d'exercer un droit ou de bénéficier d'un service ou d'un contrat**».
L'annexe I des lignes directrices met à disposition des exemples de cadres **spécifiques en fonction des secteurs**, tels que le «**Modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure**», disponible en anglais à l'adresse suivante: http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.
Voir en particulier les pages 27 à 31 relatives à l'**identification, la quantification (sévérité et probabilité) et l'évaluation** du «risque».
- Enfin, voir le **projet de liste des autorités de contrôle compétentes en matière d'opérations de traitement soumises à l'obligation de réaliser une analyse d'impact sur la protection des données (article 35, paragraphe 4, du RGPD),** disponible en anglais à l'adresse suivante: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[47] Voir l'arrêt de la Cour EDH *Big Brother Watch e.a. c. Royaume-Uni*, 13 septembre 2018, point 2.43: «2.43. L'**intrusion collatérale** consiste à obtenir toute information relative à des individus autres que ceux qui font l'objet de l'enquête. La question de l'intrusion collatérale fait partie des éléments pris en considération dans le cadre du principe de proportionnalité et devient d'autant plus pertinente lorsqu'elle concerne les données relatives au trafic et les données relatives à l'utilisation du service. Les demandes doivent inclure des détails relatifs aux **intrusions collatérales qui pourraient survenir et à l'incidence qu'aurait la durée demandée sur la mesure sur ces intrusions**. Lorsque le **risque d'intrusion collatérale est minime**, par exemple lorsque les informations demandées sont les détails concernant l'abonné qui fait l'objet de l'enquête, **il convient de relever l'absence d'une telle intrusion collatérale**» (caractères gras ajoutés).

[48] Voir l'arrêt de la CJUE dans les affaires jointes C-465/00, C-138/01, et C-139/01, *Rechnungshof*, ECLI:EU:C:2003:294, point 52: «*Le gouvernement autrichien relève, en particulier, que, dans le cadre du contrôle de proportionnalité, il convient de prendre en considération **la mesure** dans laquelle les données affectent la vie privée. Aussi, des données qui touchent à **l'intimité de la personne, à la santé, à la vie familiale ou à la sexualité** doivent-elles être plus fortement protégées que des données relatives aux revenus et aux impôts qui, si elles revêtent également un caractère personnel, ne concernent que dans une moindre mesure l'identité de la personne et sont par là même moins sensibles*» (caractères gras ajoutés).
- À propos du traitement de **données relatives à la santé**, voir la page 13 de **l'avis 3/2017 du CEPD sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)**: «Le CEPD doute que le traitement de cette catégorie de données particulièrement sensibles à une si grande échelle et pour la durée définie dans la proposition réponde aux conditions fixées à l'article 52, paragraphe 1, de la charte et, dès lors, qu'il soit considéré comme nécessaire et proportionné. Le CEPD s'interroge sur la pertinence de la collecte et du traitement de données concernant la santé tels qu'envisagés dans la proposition en raison de leur manque de fiabilité, ainsi que la nécessité du traitement de

- *le **degré d'intrusion***, en s'interrogeant: *sur la nature de l'activité* sur laquelle porte la mesure (si elle affecte des activités soumises à une obligation de confidentialité telles que les relations entre un avocat et son client, les activités médicales); *sur le contexte*; sur le fait qu'il puisse s'agir en réalité de ***profilage*** des individus concernés[49]; sur le fait que le traitement puisse supposer l'utilisation de systèmes de prise de décision ***automatisés*** (entièrement ou en partie) comportant un «taux d'erreur»[50];

- si la mesure concerne des *personnes **vulnérables*** ou non[51];

---

ces données au vu du lien limité qui existe entre les risques en matière de santé publique et les voyageurs exemptés de l'obligation de visa.»

- Les risques liés à l'intelligence artificielle appliquée à la reconnaissance faciale (et à la reconnaissance des expressions) font l'objet ces derniers temps d'une attention particulière. Voir *AI Now Report 2018*, décembre 2018, disponible en anglais à l'adresse suivante: https://ainowinstitute.org/AI_Now_2018_Report.pdf.

- À propos des **données biométriques**, voir les , pages 30 et 31 de **l'avis 03/2012 du groupe de travail «article 29» sur l'évolution des technologies biométriques**, sur les risques spécifiques posés liés aux données biométriques; ainsi que **l'avis 02/2012 du groupe de travail «article 29» sur la reconnaissance faciale dans le cadre des services en ligne et mobiles**, section 5, «Risques spécifiques et recommandations».

[49] Dans ce contexte, le terme «profilage» est entendu au sens large, à savoir «élaboration du profil de l'individu», tel qu'il est défini dans l'affaire *Tele2*, et non nécessairement dans l'acception de l'article 4, paragraphe 4, du RGPD: «"*profilage": toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne*».

[50]Au sujet de l'automatisation des décisions, voir l'avis 1/15 de la CJUE, ECLI:EU:C:2017:592, sur le projet d'accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens. Dans son avis, la Cour relève que le système canadien d'évaluation des risques relatifs aux voyageurs de l'Union européenne fonctionne de manière systématique et automatisée, **avec en outre un taux d'erreur «non négligeable»** qui expose de nombreux individus ne posant aucun risque à une surveillance continue de la part de l'Agence des services frontaliers du Canada et d'autres agences. La Cour insiste sur le fait que les systèmes algorithmiques et les technologies d'évaluation des risques doivent être «utilisés de manière **non discriminatoire**» et que les décisions finales doivent «être fondées uniquement et résolument sur une appréciation individualisée **humaine**». En l'espèce, on remarque également que les droits à la vie privée et à la protection des données à caractère personnel peuvent être liés à d'autres droits fondamentaux et principes fondamentaux (ici, la non-discrimination).

- Plus particulièrement, à propos de l'**incidence des systèmes de prise de décision automatisés utilisés par les États ou les autorités publiques**, voir le document édité par le gouvernement australien, *Automated Assistance in Administrative Decision Making, Better Practice Guide*, février 2007 (bien qu'il n'ait pas été mis à jour, il contient un certain nombre de questions pertinentes), disponible à l'adresse suivante: https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf.

[51] Cour EDH,*S.et Marper*, point 124: «La Cour estime en outre que la conservation de données relatives à des personnes non condamnées peut être **particulièrement préjudiciable** dans le cas de **mineurs**, tel le premier requérant, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société.»

- Voir, à titre d'exemple relatif à l'attention particulière requise pour le traitement des données à caractère personnel concernant des mineurs, la page 2 de la **réponse du CEPD à la consultation publique de la Commission sur l'abaissement de 12 à 6 ans de l'âge des enfants pour le relevé des empreintes digitales dans le cadre de la procédure de visa**, 9 novembre 2017: «Le CEPD recommande que la nécessité et la proportionnalité de la collecte des **données dactyloscopiques d'enfants** plus jeunes fassent l'objet d'une **réflexion et d'une évaluation préalables supplémentaires dans le cadre de l'analyse d'impact** réalisée pour accompagner la future proposition de la Commission concernant la révision du règlement VIS.» La réponse du CEPD est disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-11-09_formal_comments_2017-0809_fr.pdf.

- si la mesure **porte également sur *d'autres droits fondamentaux*** (il pourrait s'agir de droits fondamentaux «liés inextricablement»[52], tels que le droit à la protection de la vie privée et le droit à la libre expression, comme dans les affaires *Digital Rights* et *Tele2* jugées par la CJUE).

Dans les cas où il n'est pas possible de déterminer en amont certaines des incidences, il peut être utile d'appliquer le **principe de précaution**[53]. À titre d'illustration de la manière dont ce principe peut être appliqué, il pourrait être suggéré au législateur, en fonction de toutes les circonstances pertinentes de l'espèce, d'adopter une «approche incrémentielle», c'est-à-dire de choisir d'utiliser un outil informatique déjà *expérimenté et vérifié* plutôt qu'un outil informatique dont l'efficacité (faux négatifs, faux positifs) n'a pas encore été testée de manière approfondie.

Exemples pertinents

EXEMPLE 1: *Tele2 Sverige AB* (CJUE, C-203/15 et C-698/15, ECLI:EU:C:2016:970)

La Cour estime que l'**ingérence** est **sérieuse**, en particulier à la lumière du fait que les mesures supposent que soit établi un profil de l'intéressé.

[52] Voir C. Docksey, «*Four fundamental rights: finding the balance*», International Data Privacy Law, 2016, Vol. 6, nº 3, page 203: «[D]ans certains contextes, tels que ceux de la surveillance de masse et de la réglementation indépendante, les droits au respect de la vie privée, à la protection des données et à la liberté d'expression fonctionnent de manière totalement complémentaire et se renforcent mutuellement.»

[53] Hans Jonas a été le précurseur du principe de précaution dès les années 1970. Le 2 février 2000, la **Commission européenne** affirmait dans sa **communication sur le recours au principe de précaution** (COM(2000) 1 final): «Bien que dans le Traité le principe de précaution ne soit expressément mentionné que dans le domaine de l'**environnement**, son champ d'application est **beaucoup plus large**. Il couvre les circonstances particulières **où les données scientifiques sont insuffisantes, peu concluantes ou incertaines**, mais où, selon des indications découlant d'une évaluation scientifique objective et préliminaire, il y a des **motifs raisonnables de s'inquiéter** que les effets potentiellement dangereux sur l'environnement et la santé humaine, animale ou végétale soient incompatibles avec le niveau choisi de protection.» La communication est disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1580025959964&uri=CELEX:52000DC0001.
Nous estimons que ce principe, tout comme la métaphore de la «pollution des données» pour la perte de vie privée, est également applicable aux risques pour la vie privée et pour la protection des données à caractère personnel.
- «Lorsqu'il n'existe pas de consensus concernant le développement de nouvelles technologies s'immisçant dans la vie privée, la Cour EDH fait reposer sur un État membre "revendiquant un rôle de pionnier" la "responsabilité particulière de trouver un juste équilibre"», P. Popelier et C. Van De Heyning, *Procedural Rationality: Giving Teeth to the Proportionality Analysis*, European Constitutional Law Review, 9, 2013, page 243, en référence à l'affaire *S. et Marper c. Royaume-Uni*, Cour EDH.
- IDans son **avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE**, le CEPD a tenu compte des risques imprévisibles et a par conséquent appelé à un débat plus large (sur l'interopérabilité), fondé sur des éléments factuels: *«[...] L'interopérabilité n'est pas essentiellement un choix technique, c'est avant tout un choix politique à faire, qui aura des **implications juridiques et sociétales importantes dans les années à venir**. Dans le contexte d'une tendance claire consistant à mélanger des objectifs législatifs et politiques communautaires distincts (c'est-à-dire contrôles aux frontières, asile et immigration, coopération policière et, désormais aussi, judiciaire en matière pénale), ainsi qu'à assurer aux services répressifs un accès systématique aux bases de données à finalité non répressive, la décision du législateur de l'UE de rendre les systèmes informatiques à grande échelle interopérables aurait non seulement une incidence profonde et durable sur leur structure et leur mode de fonctionnement, mais modifierait également la façon dont les principes juridiques ont été interprétés dans ce domaine jusqu'à présent, marquant ainsi un "point de non-retour". Pour ces raisons, le CEPD appelle à un **débat plus large sur l'avenir de l'échange d'informations au sein de l'UE, sur sa gouvernance et sur les moyens de sauvegarder les droits fondamentaux dans ce contexte**.*» (point 25).

La Cour relève que: «*[la législation] prévoit une* ***conservation généralisée et indifférenciée*** *de* ***l'ensemble des données relatives au trafic et des données de localisation*** *de* ***tous les abonnés et utilisateurs inscrits*** *concernant* ***tous les moyens de communication électronique****, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Ainsi qu'il ressort de la décision de renvoi, les* ***catégories de données*** *visées par cette réglementation correspondent, en substance, à celles dont la conservation était prévue par la directive 2006/24.*»

«*Les* ***données*** *que doivent ainsi conserver les fournisseurs de services de communications électroniques* ***permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile****. Au nombre de ces données figurent, notamment, le* ***nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services [i]nternet****. Ces données* ***permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu****. En outre, elles permettent de connaître la* ***fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée*** *(voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 26).*»

«***Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci*** *(voir, par analogie, en ce qui concerne la directive 2006/24, l'arrêt Digital Rights, point 27). En particulier, ces données fournissent les moyens d'****établir [...] le profil des personnes concernées****, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.*»

«*L'****ingérence que comporte une telle réglementation*** *dans les droits fondamentaux consacrés aux articles 7 et 8 de la [c]harte s'avère* ***d'une vaste ampleur*** *et doit être considérée comme* ***particulièrement grave****. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées* ***le sentiment que leur vie privée fait l'objet d'une surveillance constante*** *(voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37).*»

*À propos de l'incidence de la mesure sur d'****autres droits fondamentaux*** *liés aux droits à la vie privée et à la protection des données à caractère personnel, la Cour relève que: «la conservation des données relatives au trafic et des données de localisation pourrait [...] avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur* ***liberté d'expression****, garantie à l'article 11 de la charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28)*» (caractères gras ajoutés)».

La Cour prend également en considération l'incidence de la mesure *ratione personae*, à savoir l'obligation imposée par la législation de conserver et de rendre accessibles (également) des données relatives aux **membres de professions bénéficiant d'informations protégées par le secret professionnel ou autrement confidentielles**: «*une attention particulière doit [...] être accordée à la nécessité et à la proportionnalité lorsque les données relatives à des communications demandées se rapportent à une personne qui est membre d'une profession bénéficiant d'informations protégées par le secret professionnel ou autrement confidentielles*» (caractères gras ajoutés).

EXEMPLE 2: *Ministerio Fiscal* (CJUE, C-207/16, ECLI:EU:C:2018:788)

La Cour juge que: «*Il convient [...] de* ***déterminer si****, en l'occurrence, en fonction des circonstances de l'espèce,* ***l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la [c]harte*** *qu'un*

accès de la police judiciaire aux données en cause au principal comporterait ***doit être considérée comme étant "grave"****.*»

«*À cet égard,* ***la demande en cause au principal*** *par laquelle la police judiciaire sollicite, pour les besoins d'une enquête pénale, l'autorisation judiciaire d'accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques, a pour seul objet d'identifier les titulaires des cartes SIM activées, pendant une période de douze jours, avec le code IMEI du téléphone mobile volé. [...] cette demande vise l'accès aux* ***seuls*** *numéros de téléphone correspondant à ces cartes SIM ainsi qu'aux données relatives à l'identité civile des titulaires desdites cartes, telles que leurs nom, prénom et, le cas échéant, adresse. En revanche,* ***ces données ne portent pas [...] sur*** *les* ***communications effectuées avec le téléphone mobile volé ni sur la localisation de celui-ci.»***

«*Il apparaît donc que les données visées par la demande d'accès en cause au principal permettent uniquement de mettre en relation, pendant une période déterminée, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation,* ***ces données ne permettent de connaître ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée. Lesdites données ne permettent donc pas de tirer de conclusions précises concernant la vie privée des personnes dont les données sont concernées.***» (caractères gras ajoutés).

La Cour se fonde sur ces considérations pour juger que l'**ingérence ne saurait être qualifiée de grave**. On observe qu'un des éléments essentiels retenus par la Cour pour estimer que l'ingérence n'était «pas grave» (à cet égard, le raisonnement est à l'opposé de celui de l'arrêt *Tele2*) est **l'absence de volonté d'établir un profil de l'individu concerné**.

EXEMPLE 3: Avis 1/15 de la CJUE sur l'*accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens (PNR)* (ECLI:EU:C:2017:592)

Dans l'affaire «PNR Canada», la Cour évalue l'**ingérence** en examinant tout particulièrement la mesure, le degré d'intrusion et la portée du projet d'accord *ratione personae*. Elle considère notamment que cette dernière - la portée - constitue un problème (parmi d'autres aspects). La Cour estime que «*[s]i l'ingérence que comporte l'accord envisagé est* ***moins vaste*** *que celle prévue par* la directive 2006/24 tout en étant également **moins intrusive** dans la vie quotidienne de chaque personne, son **caractère indifférencié et généralisé** suscite des interrogations» (caractères gras ajoutés).

La Cour relève d'autres questions problématiques: (i) l'identification de l'autorité compétente responsable du traitement des données; (ii) le traitement automatisé (absence de garanties relevée aux points 258 à 260); (iii) les conditions d'accès aux données conservées par les autorités répressives; (iv) la durée de conservation des données; (v) la divulgation et le transfert de données; (vi) la surveillance par une autorité indépendante. La CJUE relève *également* les mêmes problèmes dans les affaires *Digital Rights* et *Tele2*.

EXEMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJUE, C-473/16, ECLI:EU:C:2018:36)

À propos de **l'ingérence** provoquée par la mesure examinée, la Cour observe que: «*l'****ingérence*** *dans la vie privée du demandeur de protection internationale constituée par la réalisation et l'utilisation d'une expertise, telle que celle en cause au principal, présente, au regard de la nature et de l'objet de celle-ci, une* ***gravité particulière***».

«*[U]ne telle expertise repose notamment sur le fait que la personne concernée* ***se soumet à une série de tests psychologiques*** *destinés à établir un élément essentiel de l'identité de cette personne qui a trait à sa sphère personnelle en tant qu'il se rapporte à des* ***aspects intimes de la vie de ladite personne*** *[...]*.»

«*Il y a également lieu de tenir compte, en vue d'apprécier la* ***gravité de l'ingérence*** *constituée par la réalisation et l'utilisation d'une expertise psychologique telle que celle en cause au principal du principe 18 des principes de Yogyakarta sur l'application de la législation internationale des droits humains en matière d'orientation sexuelle et d'identité de genre, auquel se sont référés les gouvernements français et néerlandais, qui précise notamment que nul ne peut être forcé de subir une quelconque forme de test psychologique en raison de son orientation sexuelle ou de son identité de genre*.»

«*Il ressort de la combinaison de ces éléments que* ***la gravité de l'ingérence*** *dans la vie privée constituée par la réalisation et l'utilisation d'une expertise, telle que celle en cause au principal, dépasse ce qu'impliquent l'évaluation des déclarations du demandeur de protection internationale relatives à une crainte de persécution en raison de son orientation sexuelle ou le recours à une expertise psychologique ayant un autre objet que celui d'établir l'orientation sexuelle de ce demandeur*» (caractères gras ajoutés).

EXEMPLE 5: Avis 06/2016 du CEPD sur le deuxième train de mesures «Frontières intelligentes» de l'Union européenne[54]

«Le CEPD souhaite tout d'abord souligner que, sous l'angle des articles 7 et 8 de la [c]harte**, le traitement des données à caractère personnel entraîné par le système proposé d'entrée/sortie est important et intrusif**, compte tenu du **nombre de personnes concernées** par ce système, du **type d'informations** traitées, **des moyens utilisés** à cet effet et des différentes finalités poursuivies, comme expliqué ci-dessous.»

EXEMPLE 6: Avis du CEPD 3/2017 sur la proposition de règlement portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS)

«La proposition prévoit l'évaluation de toutes les demandes introduites par des ressortissants de pays tiers exemptés de l'obligation de visa au regard des règles d'examen de l'ETIAS, alors que seul un nombre restreint d'entre eux est réellement susceptible de poser certains types de risques et de se voir refuser une autorisation de voyage. Ces opérations automatisées et non transparentes de traitement de données à caractère personnel entraînent en tant que telles une **ingérence non négligeable** dans les droits fondamentaux d'un **nombre illimité de demandeurs**, qui seront **soumis à un profilage**; il convient de rechercher un équilibre entre cette ingérence et les résultats escomptés de ce type d'outil.

En outre, en fonction de la **méthode utilisée** pour déterminer les indicateurs de risques spécifiques, que l'on peut interpréter dans un sens très large, **le nombre de personnes qui se verraient refuser une autorisation automatique en raison d'une réponse positive se fondant sur les règles d'examen risque d'être relativement élevé**, alors que ces personnes ne présentent en réalité aucun risque.»

[54] Disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/16-09-21_smart_borders_fr.pdf.

Étape 3: déterminer si la mesure atteint un «juste équilibre»

Si (et uniquement si) le législateur a réuni **l'ensemble des informations requises** et réalisé l'évaluation de l'importance, de l'efficacité et de l'efficience de la mesure et de son ingérence dans la vie privée et dans la protection des données à caractère personnel, il doit déterminer quel est le juste équilibre entre ces deux aspects.

Si les **informations sont asymétriques**, par exemple si les bénéfices sont connus, mais que les coûts sont inconnus, ou *vice-versa*, il s'avérera difficile, voire impossible, de déterminer si la mesure est proportionnée, en tenant compte de l'ensemble des facteurs.

En pratique, le principe de proportionnalité exige que soit trouvé un **équilibre** entre la mesure et la nature de l'ingérence, d'une part, et les motifs de cette ingérence (les besoins), traduits en objectifs effectivement poursuivis par la mesure, d'autre part. La CJUE a souligné que *«[l]orsque plusieurs droits et libertés fondamentaux protégés par l'ordre juridique de l'Union sont en cause, l'appréciation de l'éventuel caractère disproportionné d'une disposition du droit de l'Union doit s'effectuer dans le respect de la* ***conciliation nécessaire des exigences*** *liées à la protection de ces différents droits et libertés et d'un* ***juste équilibre*** *entre eux*»[55].

En d'autres termes, le principe sert d'instrument pour mettre en balance des intérêts opposés selon des critères rationnels dans les cas où aucun de ces intérêts ne l'emporte *a priori*[56].

En pratique, il existe une méthode permettant de déterminer si un acte juridique de l'Union peut être jugé compatible avec les articles 7 et 8 de la charte ainsi qu'avec le principe de proportionnalité visé à l'article 52, paragraphe 1, de la charte. Cette méthode est entre autre inspirée des arrêts de la CJUE cités dans les présentes lignes directrices, notamment, mais non exclusivement, dans le domaine spécifique des «programmes généraux de surveillance»[57].

---

[55] Affaires de la CJUE C-283/11, *Sky Österreich GmbH/Österreichischer Rundfunk* [GC], ECLI:EU:C:2013:28, point 60; C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, ECLI:EU:C:2008:54, points 65 et 66; et C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, point 47; arrêt de la Cour EDH , *Big Brother Watch e.a. c. Royaume-Uni*, 13 septembre 2018, «2.42. Tout examen de la proportionnalité de la demande doit tout particulièrement prendre en considération les droits de l'individu (notamment le droit à la vie privée et, le cas échéant, à la libre expression) et s'attacher à mettre ceux-ci en balance face au bénéfice pour l'enquête.»

[56] Voir, en particulier, l'affaire C-28/08 de la CJUE, *Bavarian Lager*, point 56: «*Les règlements nº 45/2001 et nº 1049/2001 ont été adoptés à des dates très rapprochées. Ils ne comportent pas de dispositions prévoyant expressément la primauté de l'un des règlements sur l'autre*.»

[57] À la page 12 de son **avis 4/2018 sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE**, le CEPD a précisé que «les nouvelles opérations de traitement des données **ayant pour but d'identifier correctement les personnes concernées** constituent **une atteinte aux droits fondamentaux protégés par les articles 7 et 8 de la charte**. Par conséquent, elles doivent satisfaire aux critères de nécessité et de proportionnalité (article 52, paragraphe 1, de la charte).»

- Voir également *S. et Marper c. Royaume-Uni*, Cour EDH, point 67: «Le **simple fait de mémoriser des données relatives à la vie privée d'un individu** constitue une ingérence au sens de l'article 8 [...]. Peu importe que les informations mémorisées soient ou non utilisées par la suite [...]. Toutefois, pour déterminer si les informations à caractère personnel conservées par les autorités font entrer en jeu l'un des aspects de la vie privée précités, la Cour tiendra dûment compte du contexte particulier dans lequel ces informations ont été recueillies et conservées, de la nature des données consignées, de la manière dont elles sont utilisées et traitées et des résultats qui peuvent en être tirés.»

Procédure à suivre

- Premièrement, *avant même* la mise en balance, vérifier s'il y a **asymétrie des informations**: *toutes les informations pertinentes ont-elles été réunies? Les «bénéfices» et les «coûts» de la mesure ont-ils tous deux fait l'objet d'un examen?*
- Ensuite, **comparer** les contraintes engendrées pour la vie privée et la protection des données avec les bénéfices (la mise en **balance**): *compte tenu des restrictions engendrées pour les droits à la vie privée et à la protection des données, les mesures envisagées pour parvenir à l'objectif constituent-elles une réponse proportionnée au besoin sur lequel est fondée la proposition de législation?*
- Une fois la mise en balance effectuée, s'assurer que des **éléments de preuve** pertinents sont produits et, le cas échéant, publiés, confirmant que **l'analyse a bien été réalisée** (au moyen d'un *rapport sur le critère de la proportionnalité*, c'est-à-dire une analyse synthétique des **résultats** de l'évaluation réalisée).
- **Conserver (consigner et enregistrer) tous les documents pertinents** obtenus ou produits lors de la mise en **balance** et de l'élaboration du *rapport relatif au critère de proportionnalité*. Cette documentation doit être pertinente et suffisamment complète pour justifier la mesure examinée, objet de l'évaluation (ou pour en relever les problèmes les plus importants), et référencée en annexe du rapport[58].

---

[58] Dans ses conclusions relatives aux affaires jointes C-293/12 et C-594/12 (*Digital Rights*, ECLI:EU:C:2013:845), l'avocat général a défini l'**absence de justification pertinente et suffisante** à la **durée de conservation des données de deux ans** prévue par la directive comme l'un des arguments essentiels ayant emporté sa conviction que cette durée de conservation n'était pas proportionnée (par rapport à une durée de conservation inférieure à un an, considérée comme justifiée). Voir les points 148 et 149: «*[I]l peut être considéré qu'une durée de conservation de données personnelles "qui se mesure en mois" est à bien différencier d'une durée "qui se mesure en années"». La première correspondrait à celle qui se situe dans la vie qui se perçoit comme présente et la seconde à celle qui se situe dans la vie qui se perçoit comme mémoire. L'ingérence dans le droit au respect de la vie privée est, dans cette perspective, chaque fois différente et la nécessité de chacune de ces ingérences doit pouvoir être justifiée. Or, si la nécessité de l'ingérence dans la dimension du temps présent apparaît comme suffisamment justifiée, je n'ai trouvé* ***aucune justification à une ingérence devant s'étendre dans le temps historique****. Exprimé plus directement, et sans nier qu'il y ait des activités criminelles qui se préparent longtemps à l'avance, je n'ai trouvé, dans les différentes prises de position défendant la proportionnalité de l'article 6 de la directive 2006/24, aucune justification suffisante pour que la durée de conservation des données à établir par les États membres doive ne pas demeurer dans une limite inférieure à une année.*»

- Voir également les affaires jointes *Volker und Markus Schecke et Hartmut Eifert*, **C-92/09 et C-93/09**, ECLI:EU:C:2010:662, point 81: «***En effet, rien n'indique*** *que le Conseil et la Commission ont pris en considération, lors de l'adoption de l'article 44 bis du règlement nº 1290/2005 et du règlement nº 259/2008, des modalités de publication d'informations relatives aux bénéficiaires concernés qui seraient conformes à l'objectif d'une telle publication tout en étant moins attentatoires au droit de ces bénéficiaires au respect de leur vie privée, en général, et à la protection de leurs données à caractère personnel, en particulier [...].*» (caractères gras ajoutés).

- À la page 3 de son **avis 7/2018** sur la proposition de règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et d'autres documents, 10 août 2018 (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_fr_0.pdf), le CEPD «[...] *fait observer que l'analyse d'impact accompagnant la proposition* ***ne semble pas soutenir l'option stratégique retenue*** *par la Commission, à savoir l'intégration obligatoire d'images faciales et de deux empreintes digitales dans les cartes d'identité (et les titres de séjour). (...) Par conséquent, le CEPD recommande de réévaluer la nécessité et la proportionnalité du traitement des données biométriques (image faciale combinée aux empreintes digitales) dans ce cadre.*»

- Dans le même ordre d'idées, à la page 3 de son **avis 7/2017 sur la nouvelle base juridique du système d'information Schengen** du 2 mai 2017 (disponible à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/17-05-02_sis_ii_opinion_fr.pdf), le CEPD a estimé que «[...] *l'introduction de nouvelles catégories de données, et notamment de nouveaux identifiants biométriques, soulève*

Exemples pertinents

EXEMPLE 1: *Tele2 Sverige AB* (CJUE, C-203/15 et C-698/15, ECLI:EU:C:2016:970)

Dans l'arrêt *Tele2*, la Cour juge que: «*[e]u égard à la* ***gravité*** *de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de localisation,* ***seule la lutte contre la criminalité grave*** *est susceptible de justifier une telle mesure [...]*» (caractères gras ajoutés).

La Cour avait clairement à l'esprit, d'une part, l'importance et l'efficacité de la mesure et, d'autre part, la **portée** (non limitée aux données correspondant à une période donnée et/ou à une zone géographique et/ou à des personnes susceptibles d'être impliquées dans des formes de criminalité grave) et le **degré/l'intensité** (notamment par le **profilage**) de l'ingérence.

Après avoir mesuré les deux versants l'un par rapport à l'autre, la Cour conclut que: «*[l]'efficacité de la lutte contre la criminalité grave [...]* ***ne saurait à [elle seule] justifier*** *qu'une réglementation nationale prévoyant la* ***conservation généralisée et indifférenciée*** *de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte.*» La mesure «***excède donc les limites du strict nécessaire*** *et ne saurait être considérée comme étant justifiée, dans une société démocratique*» (caractères gras ajoutés).

EXEMPLE 2: *Ministerio Fiscal* (CJUE, C-207/16, ECLI:EU:C:2018:788)

Dans l'affaire *Ministerio Fiscal*, la Cour conclut que la mesure examinée est **proportionnée** (c'est-à-dire qu'elle satisfaisait au critère de la proportionnalité et était, partant, légale au regard des principes de nécessité et de proportionnalité).

Dans le cadre de l'évaluation en question, un des éléments essentiels est constitué par le fait que l'ingérence n'est «pas grave» et ne l'emporte donc pas sur l'importance («également» raisonnable) de l'objectif que la mesure permet d'atteindre.

Selon la Cour, «*lorsque* ***l'ingérence*** *que comporte un tel accès n'est* ***pas grave****, ledit accès est susceptible d'être* ***justifié par un objectif de prévention, de recherche, de détection et de poursuite d'"infractions pénales" en général***.» En revanche, «conformément au principe de proportionnalité, une ingérence **grave** ne **peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales**, que **par un objectif de lutte contre la criminalité devant également être qualifiée de "grave"**».(caractères gras ajoutés)

EXEMPLE 3: Avis 1/15 de la CJUE sur l'*accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens (PNR)* (ECLI:EU:C:2017:592)

La mesure faisant l'objet du recours en l'espèce est telle qu'elle présente une **asymétrie d'informations** entre les bénéfices escomptés et l'incidence sur les droits fondamentaux à la vie privée et à la protection des données à caractère personnel. Cette asymétrie est notamment due au fait que **les catégories de données à caractère personnel** destinées à être traitées ne sont pas définies **clairement et précisément**; la mesure **ne définit pas** non plus les règles applicables au contrôle préalable des passagers.

En effet, l'absence de précisions rend non seulement l'exercice de comparaison impossible, elle amène également la Cour à déclarer d'emblée l'accord, dans la version présentée, **incompatible** avec les articles 7 et 8 et l'article 52, paragraphe 1, de la charte.

---

la question de la nécessité et de la proportionnalité des changements proposés, et, par conséquent, les propositions devraient être complétées par l'analyse d'impact sur le droit au respect de la vie privée et le droit à la protection des données consacrés par la [c]harte des droits fondamentaux de l'Union européenne.»

EXEMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJUE, C-473/16, ECLI:EU:C:2018:36)

Dans cette affaire, la Cour prend en considération l'ensemble des éléments relatifs à l'importance et à l'efficacité de la mesure, d'une part, et à l'ingérence qu'elle suppose (en l'espèce, à l'encontre d'une personne précise), d'autre part, pour conclure que: «*[L]'article 4 de la directive 2011/95, lu à la lumière de l'article 7 de la charte, doit être interprété en ce sens qu'il* ***s'oppose à la réalisation et à l'utilisation, en vue d'apprécier la réalité de l'orientation sexuelle alléguée d'un demandeur de protection internationale, d'une expertise psychologique****, telle que celle en cause au principal, qui a pour objet, sur la base de tests projectifs de la personnalité, de fournir une image de l'orientation sexuelle de ce demandeur*» (caractères gras ajoutés).

En d'autres termes, la Cour estime que la mesure en cause n'est **pas proportionnée** en raison de l'ingérence extrêmement grave qu'elle constitue, mais également en raison de son absence d'efficacité au regard de l'objectif recherché.

EXEMPLE 5: *Scarlet Extended* (CJUE C-70/10, ECLI:EU:C:2011:771)

Cette affaire présente l'intérêt de montrer que le **droit à la protection des données à caractère personnel** peut jouer le rôle de *droit concordant*, soit un droit qui, tout en n'étant pas le droit le plus affecté par la mesure, n'en est pas moins, **concomitamment** avec d'autres droits (tels que la liberté d'entreprise ou la liberté de recevoir ou de communiquer des informations), en mesure de faire pencher la balance pour permettre de conclure que la mesure (dont l'objectif est de mieux protéger les droits de propriété intellectuelle) n'est pas proportionnée.

Nous reproduisons les extraits les plus pertinents de cet arrêt: «*l'injonction de mettre en place le* ***système de filtrage*** *litigieux doit être considérée comme ne respectant pas l'exigence que soit assuré un* ***juste équilibre*** *entre, d'une part, la* ***protection du droit de propriété intellectuelle****, dont jouissent les titulaires de droits d'auteur, et, d'autre part, celle de la* ***liberté d'entreprise*** *dont bénéficient les opérateurs tels que les FAI.*

De plus, les effets de ladite injonction ne se limiteraient pas au FAI concerné, le système de filtrage litigieux étant ***également susceptible de porter atteinte aux droits fondamentaux des clients de ce FAI, à savoir à leur droit à la protection des données à caractère personnel*** *ainsi qu'à leur* ***liberté de recevoir ou de communiquer des informations****, ces droits étant protégés par les articles 8 et 11 de la charte.(...)*

Par conséquent, il convient de constater que, en adoptant l'injonction obligeant le FAI à mettre en place le système de filtrage litigieux, la juridiction nationale concernée ***ne respecterait pas l'exigence d'assurer un juste équilibre*** *entre le* ***droit de propriété intellectuelle****, d'une part, et la* ***liberté d'entreprise****, le* ***droit à la protection des données à caractère personnel*** *et la* ***liberté de recevoir ou de communiquer des informations****, d'autre part*» (caractères gras ajoutés).

EXEMPLE 6: Avis 1/2017 du CEPD sur la proposition de la Commission modifiant la directive (UE) 2015/849 et la directive 2009/101/CE Accès aux informations sur les bénéficiaires effectifs et conséquences sur la protection des données

Dans cet avis, tout comme dans la proposition, il est fait référence à l'objectif comme étant «un risque à éviter» (en l'espèce, le risque de blanchiment d'argent et de financement du terrorisme). En règle générale, pour être considérées comme proportionnées au but recherché, la collecte et le traitement de données à caractère personnel doivent être «ajustées» (prendre en considération) en fonction du risque (par exemple, au risque pour «l'ordre public économique») que représentent les personnes concernées. Un tel ajustement permet d'**optimiser** l'ingérence dans les droits à la vie privée et à la protection des données à caractère personnel.

Dans son avis sur la proposition de modification de la directive relative au blanchiment de capitaux, le CEPD relève que, contrairement à l'approche évoquée ci-dessus, «la proposition supprime [...] des garanties existantes qui auraient assuré un certain **degré de proportionnalité**. À titre d'exemple,

concernant l'établissement des conditions d'accès aux informations sur les transactions financières par les CRF [cellules de renseignement financier], la proposition prévoit qu'à l'avenir, les CRF puissent obtenir des informations complémentaires **non seulement sur la base de transactions suspectes** (comme c'est le cas actuellement), mais également sur la base d'une analyse ou de renseignements propres à la CRF elle-même, **même sans déclaration de transaction suspecte établie au préalable**. Le rôle des CRF change dès lors, passant d'un système «*fondé sur des enquêtes*» à un système «*fondé sur le renseignement*». Cette deuxième optique se rapproche davantage de l'exploration de données que d'une enquête ciblée, ce qui a des conséquences évidentes en matière de protection des données à caractère personnel.»

EXEMPLE 7: Lignes directrices du CEPD relatives à la vidéosurveillance

Dans les lignes directrices du CEPD relatives à la vidéosurveillance, la même approche consistant à chercher à **optimiser l'ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel par rapport à l'objectif poursuivi par la mesure** (tel que la sécurité des locaux) est utilisée: «Moyennant l'adoption d'une approche pragmatique basée sur les principes de la sélectivité et de la **proportionnalité**, les systèmes de vidéosurveillance peuvent répondre aux besoins de sécurité tout en respectant notre vie privée. Les caméras peuvent et doivent être utilisées de façon intelligente et **ne viser que des problèmes de sécurité clairement identifiés**, diminuant ainsi le plus possible la capture d'images inutiles. Cette approche permet non seulement de réduire le plus possible les atteintes à la vie privée, mais aussi d'utiliser la vidéo-surveillance d'une façon **plus ciblée et finalement plus efficace**.» Les lignes directrices proposent des recommandations spécifiques (notamment sur: l'emplacement des caméras et les angles de vue; le nombre de caméras; les horaires de surveillance; la résolution et la qualité d'image; les catégories spéciales de données; les sites sur lesquels les personnes s'attendent à un respect plus important de leur vie privée; la surveillance de haute technologie et/ou intelligente; l'interconnexion des systèmes de vidéosurveillance).

EXEMPLE 8: Avis 5/2015 du CEPD sur la proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

«Les conditions préalables essentielles au système PNR - à savoir le respect des principes de nécessité et de **proportionnalité** - ne sont toujours **pas remplies dans la proposition**. [...] [E]lle ne présente aucune analyse détaillée de la mesure dans laquelle des mesures plus respectueuses de la vie privée pourraient atteindre la finalité du système PNR de l'UE. Enfin, la collecte non ciblée et massive de données ainsi que le traitement de celles-ci dans le cadre du système PNR s'apparentent à une mesure de surveillance générale. De l'avis du CEPD, la seule finalité qui serait conforme aux exigences de transparence et de proportionnalité serait l'utilisation de données PNR au cas par cas mais uniquement en cas de menace réelle et sérieuse appuyée par des indicateurs plus spécifiques. En l'**absence d'information attestant de ce que la nécessité et la proportionnalité des mesures proposées ont été démontrées à suffisance**, le CEPD estime que la proposition, **même sous sa forme modifiée, n'est toujours pas conforme** aux normes établies aux articles 7, 8 et 52 de la [c]harte des droits fondamentaux de l'Union, à l'article 16 du TFUE et à l'article 8 de la CEDH. Le CEPD encourage les législateurs à approfondir la réflexion sur la faisabilité, compte tenu des menaces actuelles, **de mesures de surveillance plus sélectives et plus respectueuses de la vie privée sur la base d'initiatives plus spécifiques se concentrant, le cas échéant, sur des catégories ciblées de vols, passagers ou pays**.»

Étape 4: analyser les conclusions relatives à la proportionnalité de la mesure proposée. S'il est conclu que la mesure n'est «par proportionnée», déterminer et introduire des garanties de nature à la rendre proportionnée.

Si la mise en balance décrite à l'étape 3 mène à la conclusion que la mesure proposée **ne satisfait pas** à l'exigence de proportionnalité, il convient alors soit de **retirer** la mesure, soit de la **modifier** pour la rendre conforme à ces exigences.

Procédure à suivre

- Analyser de manière synthétique le **résultat** de l'évaluation menée lors de l'étape 3, tel qu'il est détaillé dans le *rapport relatif au critère de la proportionnalité*, en relevant notamment **les facteurs** ayant permis de conclure à l'absence de proportionnalité («non-satisfaction au critère de proportionnalité»);
- **Retravailler** la proposition, en élaborant si possible une ou plusieurs **possibilités de correction** qui résoudraient les problèmes les plus importants (**définir** plus précisément la finalité, les catégories et la quantité de données à caractère personnel devant faire l'objet d'un traitement[59] en vue de réduire le degré d'ingérence de la mesure dans la vie privée et la protection des données);
- Envisager et introduire des **garanties** permettant de réduire l'incidence de la proposition sur les droits fondamentaux en jeu (*par exemple*, introduire une exigence de vérification humaine s'il s'agit d'une législation prévoyant des procédures entièrement automatisées)[60].

[59] À titre d'exemple, voir **la page 3 des observations formelles du CEPD relatives à la proposition de directive du Parlement européen et du Conseil sur les gestionnaires de crédit, les acheteurs de crédit et le recouvrement de garantie**, qui recommande de mieux définir les catégories et la quantité de documents (contenant des données à caractère personnel) susceptibles de faire l'objet d'un traitement au titre de la directive. Les observations formelles sont disponibles à l'adresse suivante: https://edps.europa.eu/sites/edp/files/publication/19-01-24_comments_proposal_directive_european_parliament_fr.pdf.

[60] Des exemples de **garanties** figurent à la page 16 de l'**avis 4/2018 du CEPD sur les propositions de deux règlements portant établissement d'un cadre pour l'interopérabilité des systèmes d'information à grande échelle de l'UE**: «les différents instruments exigent également **la vérification, par une autorité indépendante**, du respect des conditions d'accès précitées avant l'accès. Dans le cas de l'ETIAS, de l'EES et du système Eurodac, les services répressifs sont également tenus de **consulter d'abord les autres systèmes pertinents** (comme les bases de données nationales, les données d'Europol, Prüm, le VIS).»
- Voir également la page 33 de l'avis de la FRA relatif à «l'interopérabilité et ses conséquences en matière de droits fondamentaux», 11 avril 2018, concernant le besoin d'accorder un traitement différencié (garanties) aux personnes vulnérables, remarques: «Le remplacement du système en cascade par un mécanisme simplifié, tel que la case "réponse positive/réponse négative" face au répertoire commun de données d'identité signifie que les données de tous les individus sont considérées comme étant toutes également sensibles et, partant, que les données des personnes en **situation de vulnérabilité** (telles que les personnes sollicitant une protection internationale) ne nécessitent pas de **garanties plus importantes**.»
- Pour ce qui est des garanties (vérification humaine, explications utiles, élaboration de rapports) dans le cadre d'une éventuelle utilisation de mesures automatisées, voir la page 8 des **observations formelles du CEPD sur la proposition de règlement du Parlement européen et du Conseil relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne**: «L'article 8, paragraphe 1, au titre des "obligations en matière de transparence", prévoit que les FSH devraient définir, dans leurs conditions commerciales, leur politique de prévention de la diffusion de contenus à caractère terroriste, "et y [joindre], **le cas échéant**, une explication pertinente du fonctionnement des mesures proactives, y compris le recours à des outils automatisés"» (caractères gras ajoutés). En outre, l'article 9, paragraphe 1, dispose que les FSH qui recourent à des procédés automatisés prévoient des garanties efficaces et adéquates pour assurer l'exactitude et le bien-fondé des décisions prises en particulier pour supprimer des contenus ou en bloquer l'accès. L'article 9, paragraphe 2, précise que ces garanties consistent notamment en "une surveillance et en des vérifications humaines, **lorsque cela se justifie**, et à tout le

- Prévoir une **réévaluation** et des **clauses de limitation dans le temps**: il est fort probable que la situation à gérer se produise dans un environnement très dynamique, tant d'un point de vue technologique que d'un point de vue sociétal. Cette incertitude peut avoir contribué à ce qu'il soit conclu que la mesure n'était «pas proportionnée» pour des motifs d'«ordre prudentiel» (le principe de précaution), en raison des incertitudes quant à l'incidence réelle de la mesure (par exemple du fait des outils technologiques envisagés). Dans ce cas, outre des garanties supplémentaires, il est conseillé de prévoir une **réévaluation** stricte (évaluations ou contrôles réguliers de l'incidence à un stade ultérieur, visant également à corriger les effets imprévus) ainsi que des **clauses de limitation dans le temps** («sauf à avoir fait l'objet d'une révision ou d'une mise en conformité, la mesure ne sera *plus applicable à compter du...*»). Il est également possible d'envisager des mécanismes ou des organismes de **contrôle spécifiques**[61].
- **Refaire** l'évaluation de la nécessité et de la proportionnalité (les deux critères, puisqu'il pourrait s'avérer nécessaire de reprendre chaque étape des premier et deuxième critères au vu des modifications apportées).

Exemples pertinents

EXEMPLE 1: *Tele2 Sverige AB* (CJUE, C-203/15 et C-698/15, ECLI:EU:C:2016:970)

Le **résultat** de l'évaluation de la proportionnalité (qualifiée, en l'espèce, de «strict nécessaire») dans l'affaire *Tele2* est **négatif**. La Cour désigne les **facteurs** qui ont motivé le résultat négatif de son évaluation: notamment, ces facteurs portent sur la relation (ou plutôt l'absence de relation) entre les données qui doivent être conservées et la menace pour la sécurité publique qu'entend contrer la mesure (voir point 106 de l'arrêt).

A contrario, la Cour définit expressément ce qu'elle entend par mesure proportionnée. La mesure, en particulier, «*doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit*

moins lorsqu'une évaluation détaillée du contexte pertinent est nécessaire [...]" (caractères gras ajoutés). Compte tenu de ces garanties, le CEPD recommande de remplacer à l'article 8, paragraphe 1, et à l'article 9, paragraphe 2, les termes «le cas échéant» et «lorsque cela se justifie» par les termes «en tout état de cause» ou, à défaut, de supprimer ces termes. Le CEPD note également que, conformément à l'article 6, paragraphe 2, les FSH devraient soumettre un rapport sur les mesures proactives qu'ils ont prises, y compris au moyen d'outils automatisés, à l'autorité compétente chargée de surveiller la mise en œuvre des mesures proactives au titre de l'article 17, paragraphe 1, point c). Le CEPD recommande de préciser au considérant 18 de la proposition que les FSH devraient fournir aux autorités compétentes toutes les informations nécessaires sur les outils automatisés utilisés afin de permettre une surveillance publique approfondie de l'efficacité de ces outils et de veiller à ce que ces derniers ne produisent pas de résultats discriminatoires, non ciblés, non spécifiques ou injustifiés. Les observations formelles sont disponibles à l'adresse suivante: https://edps.europa.eu/data-protection/our-work/publications/comments/formal-comments-edps-preventing-dissemination_fr.

[61] Voir les pages 9 et 10 du **document de travail 01/2016 du groupe de travail «article 29» sur la justification des ingérences dans les droits fondamentaux à la vie privée et à la protection des données lors du transfert de données personnelles dans le cadre de mesures de surveillance (Garanties essentielles européennes)**, WP237 du 13 avril 2016, section 6, «Garantie C: nécessité d'un mécanisme indépendant de contrôle». Le document est disponible en anglais à l'adresse suivante: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf.

limitée au strict nécessaire. En second lieu, [...] la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de ***viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave****, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un* ***critère géographique*** *lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes*» (caractères gras ajoutés).

Les points 120 à 122 détaillent d'autres **conditions** que la mesure doit respecter pour être jugée proportionnée, ainsi que des conditions relatives à l'accès aux données conservées par les autorités répressives: un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante; la signification à l'intéressé que ses données font l'objet de la mesure, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes; l'obligation de conserver les données sur le territoire de l'Union européenne; l'obligation de détruire définitivement les données au terme de la période de conservation. Ces autres conditions peuvent en réalité être considérées comme des **garanties** de nature, conjointement avec la définition de la portée de la mesure, à rendre la mesure proportionnée.

Le jugement fait en outre référence au «*contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel, un tel contrôle étant explicitement exigé à l'article 8, paragraphe 3, de la charte et constituant, conformément à la jurisprudence constante de la Cour, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel. S'il en était autrement, les personnes dont les données à caractère personnel ont été conservées seraient privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs données (voir, en ce sens, arrêts Digital Rights, point 68, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, points 41 et 58)*» (caractères gras ajoutés). Cette dernière exigence est un élément de la condition de **respect du contenu essentiel du droit fondamental** et relève du **premier critère (critère de nécessité)**.

À ce jour, le législateur **n'a *pas* présenté de nouvelle proposition** de directive relative à la conservation des données. S'il décidait de le faire, il devrait procéder à l'examen des premier et deuxième critères, soit les critères de nécessité et de proportionnalité.

EXEMPLE 2: *Ministerio Fiscal* (CJUE, C-207/16, ECLI:EU:C:2018:788)

Dans l'affaire *Ministerio Fiscal*, la Cour juge la mesure **proportionnée** à sa finalité. Elle ne relève aucun problème majeur dont le législateur devrait tenir compte. Dès lors, il est inutile de retravailler la mesure (en redéfinir l'objectif, la portée, le degré d'ingérence, prévoir davantage de garanties ou des garanties différentes) et/ou de **refaire** l'évaluation de la nécessité et de la proportionnalité.

EXEMPLE 3: Avis 1/15 de la CJUE sur l'*accord entre le Canada et l'Union européenne sur le transfert des données des passagers aériens (PNR)* (ECLI:EU:C:2017:592)

La Cour considère que la mesure n'est **pas** compatible avec les articles 7 et 8 et avec l'article 52, paragraphe 1, de la charte. Les éléments ayant motivé cette conclusion concernent essentiellement le manque de clarté et de précision de la mesure (et, partant, l'impossibilité d'en mesurer l'incidence), d'une part, et l'absence de garanties (telles que le contrôle par une autorité indépendante), d'autre part.

Dans le même temps, la Cour **détaille les conditions** (précédées par les termes «*à condition que*», «*pour autant que*») grâce auxquelles la mesure est proportionnée. D'un côté, donc, le pouvoir discrétionnaire du législateur se trouve, en l'espèce, relativement réduit, puisqu'il devra suivre à la lettre les instructions de la Cour. De l'autre côté, le travail du législateur s'en trouve clairement facilité puisqu'en suivant les indications de la Cour, il devrait s'épargner le risque de voir son texte de nouveau déclaré incompatible par la Cour.

EXEMPLE 4: *Bevándorlási és Állampolgársági Hivatal* (CJUE, C-473/16, ECLI:EU:C:2018:36)

La Cour estime qu'il faut interpréter l'article 7 de la charte en ce sens qu'il **s'oppose** à la réalisation et à l'utilisation, en vue d'apprécier la réalité de l'orientation sexuelle alléguée d'un demandeur de protection internationale, d'une expertise psychologique, telle que celle en cause au principal, qui a pour objet, sur la base de tests projectifs de la personnalité, de fournir une image de l'orientation sexuelle de ce demandeur.

Dans cette affaire, il semble difficile, compte tenu notamment de **l'intensité particulièrement forte** de l'ingérence, de prévoir des **garanties** de nature à rendre proportionné le recours à la mesure examinée.