EUROPEAN DATA PROTECTION SUPERVISOR

Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel

11 avril 2017

TABLE DES MATIÈRES

I. Objectif et mode d'utilisation du guide

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 (ci-après l'«Union»)[1]. Ces droits doivent être respectés chaque fois que les institutions et les organes de l'Union conçoivent et mettent en œuvre de nouvelles politiques ou adoptent de nouvelles mesures législatives. D'autres normes relatives aux droits fondamentaux jouent également un rôle important dans l'ordre juridique de l'Union, en particulier la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH).

Le présent guide répond aux demandes de conseils, formulées par les institutions de l'Union, sur les exigences particulières découlant de l'article 52, paragraphe 1, de la charte, en vertu duquel toute limitation de l'exercice du droit à la protection des données à caractère personnel (article 8 de la charte) doit être «nécessaire» et répondre à un objectif d'intérêt général ou au besoin de protection des droits et libertés d'autrui[2].

En même temps, 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.

La nécessité est une condition essentielle à laquelle toute proposition de mesure prévoyant le traitement de données à caractère personnel doit satisfaire.

Le présent guide a été élaboré afin d'aider à déterminer si les mesures proposées sont conformes au droit de l'Union en matière de protection des données. Il a été conçu 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 d'autres droits et libertés énoncés dans la charte.

Le CEPD respecte pleinement la responsabilité du législateur d'évaluer la nécessité et la proportionnalité d'une mesure. En conséquence, le présent guide n'entend ni ne peut fournir une évaluation définitive de la nécessité, ou de l'absence de nécessité, de toute proposition de mesure spécifique. Il fournit plutôt une liste pratique des points à vérifier, étape par étape, pour évaluer la nécessité de toute nouvelle mesure législative, ainsi qu'une analyse juridique de la notion de nécessité en ce qui concerne le traitement des données à caractère personnel.

Il complète et approfondit les orientations déjà fournies par la Commission et le Conseil sur les limitations des droits fondamentaux en général concernant, par exemple, les analyses d'impact et les contrôles de compatibilité[3].

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

Le guide se fonde sur la jurisprudence[4] de la Cour de justice de l'Union européenne (CJUE) et de la Cour européenne des droits de l'homme (CouEDH), ainsi que sur des avis antérieurs du CEPD et du groupe de travail «Article 29». Il fait suite à un document de travail[5] publié en 2016 aux fins d'une consultation publique.

Nous tenons à remercier les personnes qui nous ont fait part de leurs commentaires et nous ont ainsi permis d'améliorer le document.

Remarque sur la terminologie

En ce qui concerne les droits énoncés dans la charte des droits fondamentaux, plusieurs termes similaires, dont «limitation», «restriction», «interférence» et «portant atteinte», ainsi que leurs dérivés respectifs, sont utilisés indifféremment dans les débats stratégiques, de même que dans les textes juridiques, y compris dans la jurisprudence de la CJUE. À des fins de simplification, le présent guide respectera la terminologie de l'article 52 de la charte et utilisera en permanence le terme «limitation», sauf dans le cas des citations.

II. Analyse juridique: application du critère de la nécessité au droit à la protection des données à caractère personnel

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

L'article 8 de la charte reconnaît le droit fondamental à la protection des données à caractère personnel. Ce droit n'est pas absolu et peut être limité, à condition que les limitations respectent les exigences énoncées à l'article 52, paragraphe 1, de la charte[6]. La même analyse s'applique au droit au respect de la vie privée consacré à l'article 7 de la charte.

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 (l'objet du présent guide); et
- elle doit être proportionnelle.

Cette liste de critères définit l'ordre requis pour l'évaluation de la légalité. Tout d'abord, il convient d'examiner si une loi accessible et prévisible[7] prévoit une limitation et si le **contenu essentiel du droit** est respecté, c'est-à-dire si le droit est en effet vidé de son contenu essentiel et si la personne ne peut pas exercer le droit[8]. 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.

L'étape suivante consiste à 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. Il importe dès lors de déterminer de façon suffisamment précise l'objectif d'intérêt général afin de pouvoir évaluer la nécessité de la mesure.

Il s'agit ensuite d'évaluer la **nécessité** de la mesure législative proposée qui prévoit le traitement de données à caractère personnel.

S'il est satisfait au critère de la nécessité, la **proportionnalité** de la mesure envisagée est évaluée. Dans le cas contraire, cette évaluation est inutile. 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.

Le critère de la proportionnalité, auquel toute limitation des droits fondamentaux est soumise, sera abordé par le CEPD dans un document distinct.

Il est important de fournir **une description adéquate de la mesure**, car cette dernière peut porter atteinte à plusieurs des critères susmentionnés. En conséquence, les

juridictions peuvent parfois évaluer les critères en parallèle. Par exemple, une mesure imprécise ou définie de manière trop large peut empêcher son évaluation afin de déterminer si elle est «prévue par la loi» et «nécessaire»[9].

2. De la relation entre proportionnalité et nécessité

La **proportionnalité** est 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*»[10]. 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 la réalisation de ces objectifs*»[11]. En conséquence, elle «*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)*»[12].

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 [...]*».

Au sens large, la proportionnalité englobe à la fois la nécessité et la **pertinence** d'une mesure, c'est-à-dire la mesure dans laquelle il existe un lien logique entre la mesure et l'objectif (légitime) poursuivi. 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[13]. Ce dernier élément décrit la proportionnalité au sens strict et constitue le critère de la proportionnalité. Il doit être clairement distingué de celui de la **nécessité**.

Le 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.

La «nécessité» est également un principe de qualité des données et une condition récurrente pour presque toutes les exigences relatives à la légalité du traitement des données à caractère personnel découlant du droit dérivé de l'Union sur la protection des données[14]. Il existe également un lien entre l'article 8, paragraphe 2, de la charte et le droit dérivé, dans la mesure où l'article 8, paragraphe 2, fait référence à la base légitime pour le traitement «prévu par la loi» et que l'explication ad article 8 fait référence à ce droit dérivé en établissant que la directive 95/46/CE et le règlement (CE) nº 45/2001 «contiennent des conditions et limitations applicables à l'exercice du droit à la protection des données à caractère personnel».

Le présent guide part du principe que seule une mesure s'avérant *nécessaire* doit être soumise à un examen de la proportionnalité. 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[15]. Par exemple, une mesure de répression évaluée comme nécessaire doit ensuite être analysée de façon à déterminer si elle serait plus proportionnée si elle se limitait uniquement aux crimes graves. Un examen de la proportionnalité pourrait consister à déterminer les règles devant accompagner une mesure de surveillance avant ou après

qu'elle est autorisée. De telles règles, souvent désignées sous le terme de «garanties», permettraient de réduire les risques posés par la mesure envisagée au regard des droits fondamentaux.

Dans la pratique, un aspect spécifique d'une proposition de mesure, ou une disposition contenue en celle-ci, peut être utile à la fois pour l'évaluation de la nécessité et l'examen de la proportionnalité. Par exemple, la question de savoir si une mesure doit cibler tous les crimes ou uniquement les crimes graves peut être considérée comme une question de nécessité. En revanche, si une telle disposition était évaluée comme nécessaire, un examen de sa proportionnalité et de son risque d'éroder les valeurs d'une société démocratique resterait nécessaire. Dans la pratique, toutefois, on observe un certain chevauchement entre les notions de nécessité et de proportionnalité, et en fonction de la mesure en question, les deux examens peuvent être réalisés simultanément, voire même dans l'ordre inverse[16].

En règle générale, toutefois, il convient en premier lieu de déterminer si une limitation d'un droit fondamental est nécessaire avant de procéder à un examen de la proportionnalité.

3. De la charte et de la CEDH

Si le **droit au respect de la vie privée** (également appelé «droit à la vie privée») est reconnu par la charte (article 7) et par la CEDH (article 8), le **droit à la protection des données à caractère personnel** en tant que tel est un droit fondamental distinct inscrit dans la charte (article 8)[17].

À la suite de l'entrée en vigueur du traité de Lisbonne, la **charte** est devenue le principal instrument de référence pour déterminer si le droit dérivé de l'Union respecte les droits fondamentaux[18]. Selon une jurisprudence constante de la CJUE, la CEDH «*ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union*»[19]. En conséquence, la CJUE a affirmé dans une jurisprudence récente que l'examen de la validité d'une disposition du droit dérivé de l'Union «*doit être opéré au regard uniquement des droits fondamentaux garantis par la charte*»[20].

Cependant, conformément à l'article 6, paragraphe 3, du TUE, la CJUE a également rappelé que les dispositions de la CEDH devaient être prises en considération «*aux fins de l'interprétation*» des dispositions correspondantes de la charte[21]. En particulier, 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*». En outre, la charte elle-même dispose que dans la mesure où elle contient «*des droits correspondant à des droits garantis par la [CEDH] et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite [CEDH]*», alors que le droit de l'Union peut accorder une protection plus étendue (article 52, paragraphe 3, de la charte).

D'une part, le droit au respect de la vie privée énoncé à l'article 7 de la charte correspond directement à l'article 8 de la CEDH. D'autre part, le droit à la protection des données à caractère personnel est formulé dans la charte, mais pas dans la CEDH, et ne figure donc pas parmi les droits qui correspondent à un droit garanti par la CEDH conformément à l'article 52, paragraphe 3, de la charte[22]. Toutefois, l'explication ad article 8 de la charte

énonce que ce droit se fonde, entre autres, sur l'article 8 de la CEDH. Par conséquent, la jurisprudence de la CouEDH au titre de l'article 8 de la CEDH est pertinente, bien qu'elle ne soit pas forcément irréfutable, pour déterminer si une limitation est conforme à la charte[23]. Il existe également un dialogue constant entre la CJUE et la CouEDH, observé dans de le cadre de nombreuses références dans la jurisprudence de chacune de ces juridictions[24].

Les critères prévus à l'article 8, paragraphe 2, de la CEDH et à l'article 52, paragraphe 1, de la charte pour l'imposition d'une limitation légale au droit au respect de la vie privée sont similaires[25]. L'article 8, paragraphe 2, de la CEDH établit, en outre, que la limitation doit être nécessaire «dans une société démocratique». Bien que l'article 52, paragraphe 1, de la charte n'utilise pas le même langage, l'élément «société démocratique» est indissociable de l'ordre juridique de l'Union, étant donné qu'il découle des valeurs fondamentales de l'Union, qui comprennent le respect de la démocratie (article 2 du TUE).

En conséquence, l'article 52, paragraphe 1, et la jurisprudence de la CJUE constituent les principales références pour évaluer la nécessité des mesures limitant l'exercice des droits garantis par l'article 8 de la charte. Par ailleurs, l'analyse doit également prendre en considération les critères énoncés à l'article 8, paragraphe 2, de la CEDH, et en particulier la condition que la limitation soit nécessaire dans une société démocratique[26], telle qu'elle est interprétée par la jurisprudence de la CouEDH.

4. De la *stricte nécessité* des mesures

La jurisprudence de la CJUE applique un critère de *stricte nécessité* à toute limitation de l'exercice des droits à la protection des données à caractère personnel et au respect de la vie privée en ce qui concerne le traitement des données à caractère personnel: «*les dérogations à la protection des données à caractère personnel et les limitations de celle-ci* ***doivent s'opérer dans les limites du strict nécessaire***.» La CouEDH applique un critère de *stricte nécessité* en tenant compte du contexte et de toutes les circonstances, par exemple en ce qui concerne les mesures de surveillance secrète [27].

Il ressort de la jurisprudence de la CJUE que la condition de la stricte nécessité est de nature horizontale, quel que soit le domaine en cause, comme le secteur répressif ou commercial[28]. L'exigence de la «stricte nécessité» découle du rôle important que le traitement des données à caractère personnel suppose pour une série de droits fondamentaux, dont la liberté d'expression. Même si des réglementations spécifiques sont adoptées dans le domaine de la répression, par exemple la directive (UE) 2016/680[29], cela ne justifie pas une évaluation différente de la nécessité.

La condition de la stricte nécessité a pour autre conséquence le fait que le contrôle juridictionnel de la mesure est également strict. En d'autres termes, le pouvoir d'appréciation du législateur dans le choix de la mesure est limité. Cela étant, les conditions d'un contrôle juridictionnel strict du pouvoir d'appréciation du législateur sont également considérées parallèlement à la gravité de la limitation qu'une mesure particulière peut causer[30]. De même, le CEPD a souligné dans l'affaire pendante concernant le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers que, en raison du traitement systématique

et particulièrement intrusif des données à caractère personnel prévu dans l'accord, le contrôle juridictionnel doit être strict[31].

5. De la limitation d'un droit fondamental

L'examen de la nécessité doit être réalisé lorsque la mesure législative proposée prévoit le traitement de données à caractère personnel.

La CJUE examine les limitations à l'exercice des droits et des libertés garantis par le droit de l'Union sur la base de l'article 52, paragraphe 1, de la charte. La Cour a affirmé qu'un acte «est constituti[f] d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la charte puisqu'elle prévoit un traitement des données à caractère personnel»[32]. En principe, par conséquent, toute opération de traitement des données (collecte, conservation, utilisation ou divulgation de données) prévue par la législation constitue une limitation du droit à la protection des données à caractère personnel, que cette limitation soit ou non justifiée.

Par ailleurs, la CJUE a jugé, dans la grande majorité des affaires portant sur des actes législatifs, qu'une opération de traitement limitait à la fois le droit à la protection des données à caractère personnel et le droit au respect de la vie privée[33]. La Cour a également considéré que pour établir une limitation, «*il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients*»[34].

En ce qui concerne le droit au respect de la vie privée consacré à l'article 8 de la CEDH, la jurisprudence de la CouEDH indique que le traitement des données à caractère personnel peut constituer une limitation du droit en fonction du contexte, comme la nature sensible des données ou la manière dont elles sont utilisées[35].

6. Conclusion: la notion de nécessité dans la législation sur la protection des données, notion jurisprudentielle et factuelle qui requiert une évaluation par le législateur de l'Union

Toute proposition de mesure doit être étayée par des éléments de preuve décrivant le problème à résoudre, la façon dont il sera réglé au moyen de la mesure et les raisons pour lesquelles les mesures actuelles ou des mesures moins intrusives ne suffisent pas à le résoudre.

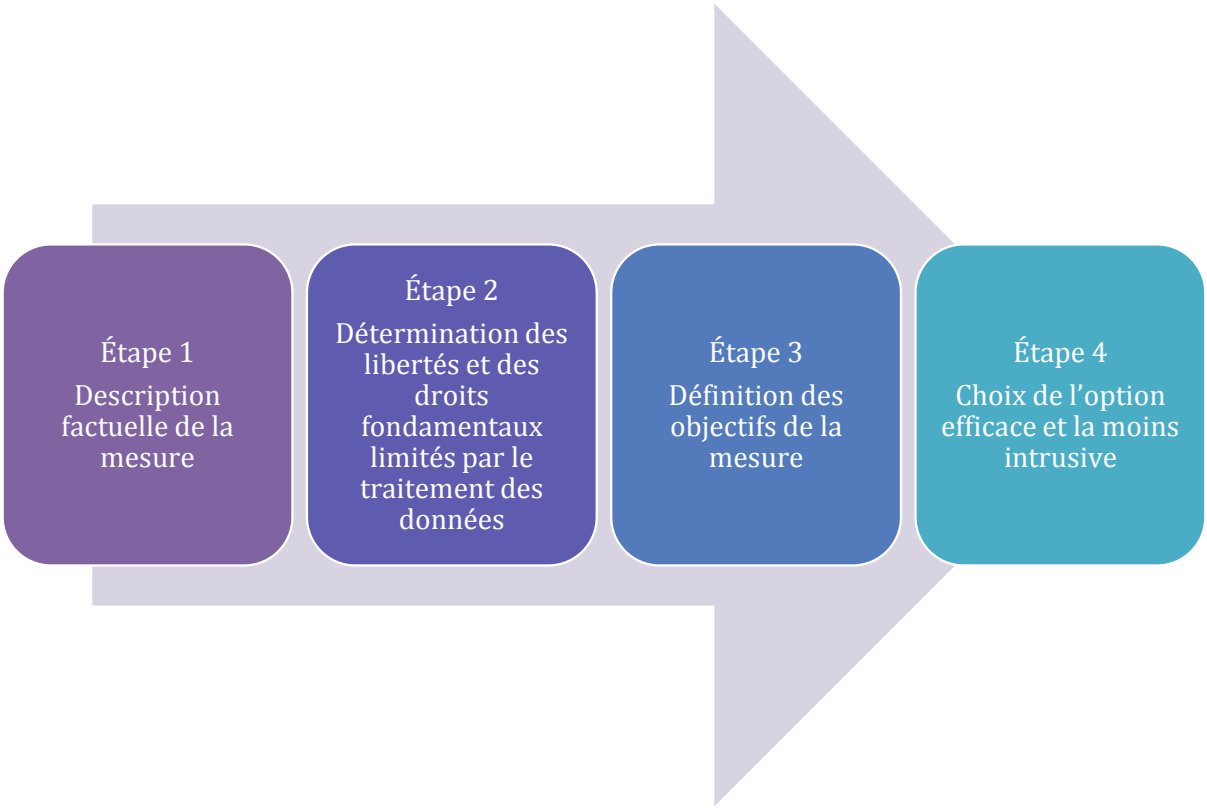
Une analyse de la jurisprudence de la CJUE et de la CouEDH indique que le critère de la nécessité prévu dans la législation sur la protection des données est une notion factuelle, et non une notion juridique purement abstraite, et que cette notion doit être examinée au regard des circonstances particulières qui entourent l'affaire, ainsi que des dispositions de la mesure et de l'objectif concret qu'elle vise à réaliser[36].

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

La liste des points à vérifier pour évaluer la nécessité consiste en quatre étapes consécutives. Chaque étape correspond à une série de questions qui faciliteront l'évaluation de la nécessité.

- 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** permettra 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»), et 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 de l'évaluation de la nécessité, la mesure devant, en particulier, être **efficace** et **la moins intrusive**.

Si l'évaluation de l'un quelconque des éléments détaillés dans les étapes 2 à 4 conduit à la conclusion qu'une mesure pourrait ne pas satisfaire à l'exigence de nécessité, alors la mesure ne doit pas être proposée, ou doit être réexaminée conformément aux résultats de l'analyse.



Étape 1: Description factuelle de la mesure proposée

Une description détaillée 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.

Conseils

- ✓ La mesure doit être suffisamment décrite pour permettre de bien comprendre sa teneur exacte et son objectif.
    - Il est particulièrement important de déterminer exactement ce que la mesure proposée prévoit en ce qui concerne le traitement des données à caractère personnel et quel(le)(s) est (sont) le(s) objectif(s) et la (les) finalité(s) concrète(s) de la mesure.
    - Comme il a été mentionné ci-dessus (section II.1), une mesure mal définie peut également avoir une incidence sur les autres conditions requises pour imposer une limitation légale aux droits fondamentaux et empêcherait de déterminer les droits auxquels il pourrait être porté atteinte.

Procédure à suivre

- ✓ **Décrire la mesure**
    - Déterminer si la mesure prévoit l'utilisation de données à caractère personnel.
        - La notion de **données à caractère personnel** est très vaste, puisque l'expression désigne «*toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*»[37]. Par conséquent, un nom, un prénom, un numéro d'immatriculation d'un véhicule, un numéro de téléphone, un numéro de passeport, une adresse IP ou tout autre identifiant unique est considéré comme une donnée à caractère personnel[38].
    - Si la mesure prévoit le traitement de données à caractère personnel, décrire:
        - l'objectif d'intérêt général poursuivi par la mesure;
        - la finalité exacte du traitement des données à caractère personnel (de façon plus détaillée que l'objectif);
        - les catégories de données;
        - les personnes dont les données seront traitées (passagers, travailleurs, migrants, etc.);

- l'entité qui traitera les données et aura accès à celles-ci (société privée, organisme public, etc.);
- les opérations de traitement envisagées (collecte, conservation, accès, transfert);
- toute autre disposition pertinente, comme la durée du traitement.

Exemples pertinents

EXEMPLE 1: Conseils du CEPD *dans le cadre de la consultation publique organisée par la Commission en 2011 (voir Conseil de l'Union européenne, doc 6370/13) sur la modification de la proposition de la Commission COM(2011) 628 final/2 pour un règlement du Parlement européen et du Conseil relatif au financement, à la gestion et au suivi de la politique agricole commune* [réglementation adoptée en vue de se conformer à l'arrêt *Schecke* sur la publication des données à caractère personnel relatives aux bénéficiaires d'aides dans le cadre de la politique agricole commune – à présent le règlement (UE) nº 1306/2013, en particulier les articles 111 à 113 et les considérants 73 à 87]

«*Le CEPD souligne qu'aux fins de l'évaluation de la conformité des exigences en matière de protection de la vie privée et des données, il est primordial d'arrêter un objectif clair et bien défini que la mesure envisagée entend servir. [...] Concernant l'objectif de contrôle, le représentant du CEPD a déclaré que la Commission devrait par conséquent indiquer clairement si l'objectif de la mesure prévoyait également d'autoriser une certaine forme de contrôle public sur les dépenses des fonds de l'Union par les bénéficiaires dont la divulgation de l'identité serait indispensable. En revanche, si l'objectif concerne uniquement le contrôle public des institutions de l'Union et de la manière dont le budget de l'Union est dépensé, il est moins évident que l'identité des bénéficiaires doive être fournie au public [...].*»

Étape 2: Détermination des libertés et des droits fondamentaux limités par le traitement des données à caractère personnel

Conseils

- ✓ Si la mesure proposée prévoit le traitement de données à caractère personnel, la mesure est constitutive d'une limitation du droit à la protection des données à caractère personnel en vertu de l'article 52, paragraphe 1, de la charte.
- ✓ En fonction de la nature des données et de la façon dont elles sont utilisées, la mesure proposée peut également limiter le droit au respect de la vie privée (également appelé «droit à la vie privée») (voir section II.5).
- ✓ À cet égard, selon une jurisprudence constante, la CJUE a affirmé que «[p]our établir l'existence d'une telle ingérence, **il importe peu que les informations communiquées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence [...]**»[39].
- ✓ Par ailleurs, la CouEDH a estimé à plusieurs reprises que la **conservation par une autorité publique de données** relatives à la vie privée d'un individu constituait

une limitation du droit au respect de sa vie privée[40], indépendamment de l'utilisation qui est faite des données[41].

- ✓ Toute opération ou tout ensemble d'opérations distincts (par exemple la collecte et une autre opération, comme la conservation de données, le transfert de données ou l'accès à des données) peut constituer des limitations séparées du droit à la protection des données à caractère personnel et, le cas échéant, du droit au respect de la vie privée. Par exemple, la CJUE a jugé que si la mesure prévoyait l'**accès des autorités nationales compétentes** aux données traitées, un tel accès constituait une ingérence supplémentaire dans le droit fondamental au respect de la vie privée[42].

- ✓ Refuser à un individu la possibilité de contester des données conservées et accessibles (c'est-à-dire le droit d'accéder aux données et de modifier celles-ci) constitue également une limitation de son droit au respect de la vie privée[43].

La mesure proposée peut également **porter atteinte à d'autres droits et libertés**, ce qui nécessite d'approfondir l'analyse. Par exemple, la mesure peut porter atteinte au droit à un recours effectif[44], au droit à la non-discrimination[45] ou au droit à la liberté d'expression[46].

- ✓ Aux termes de l'article 52, paragraphe 1, de la charte, le «**contenu essentiel**» **du droit doit être respecté** (voir section II.1). Cela signifie que la limitation ne peut pas aller jusqu'à vider le droit de ses éléments fondamentaux et donc empêcher l'exercice du droit.

Procédure à suivre

- ✓ **Déterminer si la mesure proposée prévoit, de quelque manière que ce soit, l'utilisation de données à caractère personnel. Le cas échéant, décrire:**

  - Les opérations de traitement envisagées (collecte, conservation, divulgation, transfert, etc.).
  - Les personnes/entités qui traiteront les données (entités privées, entités publiques, organismes, autorités compétentes, certains individus, etc.).
  - Les personnes/entités qui auront accès aux données.
  - La durée de conservation des données[47].
  - Les circonstances dans lesquelles les données à caractère personnel seront utilisées (sur une base systématique, uniquement dans certains cas, durant une période limitée, etc.).
  - Les personnes dont les données seront traitées (certaines catégories de personnes, utilisateurs d'un service, personnes soupçonnées d'une infraction, étrangers, ressortissants nationaux, etc.).

- ✓ **Déterminer les libertés et les droits fondamentaux qui seront limités**
    - Déterminer dans quelle mesure le traitement des données limite le droit au respect de la vie privée.
    - Détecter une possible «différence de traitement» entre les individus, susceptible de conduire à une discrimination.
    - Évaluer les conséquences sur la possibilité des individus de former un recours effectif.
    - Déterminer dans quelle mesure la liberté d'expression, la liberté de pensée et la liberté d'accès à l'information sont limitées.
    - Déterminer si le contenu essentiel des droits est limité.

Conclusions

- ✓ **Si un droit est limité**, cette simple constatation ne signifie pas que la mesure ne doit pas être proposée. En revanche, la mesure doit respecter les conditions énoncées à l'article 52, paragraphe 1, de la charte, dont celle de la nécessité.
- ✓ Si la mesure porte atteinte au **contenu essentiel du droit**, la limitation est par conséquent illégale et la mesure doit être retirée ou modifiée avant de procéder aux étapes suivantes (voir section I.1).

Exemples pertinents

EXEMPLE 2: *Huber* (CJUE, affaire C-524/06)

La Cour a évalué la légalité d'une base de données établie par les autorités allemandes, qui comprenait des données à caractère personnel sur les ressortissants de pays tiers et d'autres citoyens de l'Union qui ne possédaient pas la nationalité allemande. La Cour a conclu, entre autres, que le droit à l'absence de discrimination entre les ressortissants de l'Union devait être interprété «*en ce sens qu'il s'oppose à l'instauration par un État membre d'un système de traitement de données à caractère personnel spécifique aux citoyens de l'Union non ressortissants de cet État membre dans l'objectif de lutter contre la criminalité*» (point 81). Pour parvenir à cette conclusion, la Cour a tenu compte du fait que la lutte contre la criminalité «*vise nécessairement la poursuite des crimes et des délits commis, indépendamment de la nationalité de leurs auteurs*» (point 78). «*Partant, pour un État membre, la situation de ses ressortissants ne saurait être différente de celle des citoyens de l'Union non ressortissants de cet État membre séjournant sur son territoire au regard de l'objectif de lutte contre la criminalité.*» (point 79).

EXEMPLE 3: Avis 3/2016 du CEPD *sur les échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS),* 13 avril 2016

La proposition législative vise à mettre en place un système spécial d'échange d'informations entre les États membres sur les condamnations de ressortissants de pays tiers, qui contiendrait également des données sur les ressortissants de l'Union qui possèdent la nationalité d'un pays tiers. Ils seraient, par conséquent, traités différemment des ressortissants de l'Union qui ne possèdent pas la nationalité d'un pays tiers. Le CEPD a estimé que «*[l]a différence de traitement*

prévue dans la proposition ne semble pas nécessaire pour atteindre l'objectif poursuivi, étant donné que, pour les ressortissants de l'UE, les autorités peuvent appliquer les procédures de l'ECRIS existantes pour partager des informations» et que cette «*différence de traitement pourrait conduire à une discrimination, ce qui constituerait une violation de l'article 21, paragraphe 1, de la charte de l'UE*» (point 33).

EXEMPLE 4: *Rechnungshof* (CJUE, affaires jointes C-465/00, C-138/01 et C-139/01)

La Cour a conclu que «*la simple mémorisation par l'employeur de données nominatives relatives aux rémunérations versées à son personnel ne saurait, comme telle, constituer une ingérence dans la vie privée*». En revanche, elle a jugé que «*la communication de ces données à un tiers, en l'occurrence une autorité publique, porte atteinte au droit au respect de la vie privée des intéressés*» (point 74).

EXEMPLE 5: *Schecke* (CJUE, affaires jointes C-92/09 et C-93/09)

La publication sur l'internet des données nominatives relatives aux bénéficiaires de fonds publics et aux montants perçus par ceux-ci constitue une limitation de leur droit à la vie privée au sens de l'article 7 de la charte (point 58).

EXEMPLE 6: *Digital Rights Ireland* (CJUE, affaires jointes C-293/12 et C-594/12)

Dans le cas de la directive sur la conservation des données, la Cour a jugé que l'obligation imposée aux fournisseurs de services de communications électroniques accessibles au public ou des réseaux publics de communications de conserver, pendant une durée de six mois à deux ans, des données relatives aux communications, telles que les numéros de téléphone des appelants, les numéros de téléphone composés, les adresses de courrier électronique, les adresses IP utilisées pour accéder à l'internet, «*constitue en soi une ingérence dans les droits garantis par l'article 7 de la charte*» (point 34). «*En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental.*» (point 35). La Cour a également estimé que «la directive 2006/24/CE est constitutive d'une [limitation du] droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la charte puisqu'elle prévoit un traitement des données à caractère personnel» (point 36).

Étape 3: Définition des objectifs de la mesure

Conseils

- ✓ Conformément à l'article 52, paragraphe 1, de la charte, la mesure **doit répondre effectivement:**
  - **à des objectifs d'intérêt général reconnus par l'Union ou**
  - **au besoin de protection des droits et libertés d'autrui.**
- ✓ Les **objectifs d'intérêt général de l'Union** comprennent, par exemple, les objectifs généraux énoncés à l'article 3 ou à l'article 4, paragraphe 2, du TUE et d'autres intérêts garantis par des dispositions spécifiques des traités[48] et interprétés par la jurisprudence de la CJUE.

- L'article 23 du règlement général (UE) 2016/679 sur la protection des données comprend une liste des objectifs considérés comme légitimes pour limiter les droits de l'individu, tels que le droit d'accès aux données à caractère personnel d'un individu, et les obligations du responsable du traitement.

- La transparence et le contrôle public constituent également des objectifs légitimes (article premier et article 15, paragraphe 1, du TUE) qui permettent d'assurer une meilleure participation des citoyens au processus décisionnel[49].

✓ Les **droits d'autrui** sont en premier lieu ceux inscrits dans la charte.

- Il est peut-être nécessaire de trouver un juste équilibre entre le droit à la protection des données à caractère personnel et les autres droits, tels que les droits à une protection effective de la propriété intellectuelle, à un recours effectif, à la liberté d'expression et à l'exercice d'une activité professionnelle[50].

✓ Bien que la description de la mesure soit distincte de l'évaluation de la nécessité, elle est indispensable à la réalisation de cette dernière, car la nécessité doit être évaluée au regard du (des) objectif(s) poursuivi(s).

- Le **problème que la mesure doit résoudre**, c'est-à-dire l'objectif du traitement des données à caractère personnel, doit être précisé. Cet élément est d'autant plus important si l'on tient compte du fait qu'un objectif d'intérêt général pourrait englober différents aspects ou qu'une mesure devrait permettre de réaliser différents objectifs d'intérêt général. Par exemple, l'objectif de la protection de la sécurité publique peut être considéré comme englobant à la fois la sécurité intérieure et extérieure[51]. En conséquence, une mesure donnée doit clairement indiquer si elle couvre l'une de ces deux notions de sécurité ou chacune d'entre elles.

✓ Le problème à résoudre doit être concret, et non purement hypothétique. À cette fin, des **éléments de preuve objectifs du problème** doivent être fournis. Ces éléments de preuve peuvent consister en des faits ou des données statistiques. Ils doivent non seulement permettre une vérification scientifique, mais également convaincre de l'existence du problème.

✓ D'après la CouEDH, une **limitation sera considérée comme «nécessaire dans une société démocratique»** pour atteindre un but légitime «si elle répond à un **besoin social impérieux**». Le problème à résoudre ne doit pas seulement être réel, présent ou imminent, mais préjudiciable au bon fonctionnement de la société.

✓ Si une mesure poursuit plusieurs objectifs, une justification est nécessaire pour chacun d'eux[52].

Procédure à suivre

✓ **Déterminer et évaluer la légitimité de l'objectif poursuivi par la mesure:**

- Veiller à ce que le problème soit clairement et suffisamment décrit.

- Apporter suffisamment d'éléments de preuve scientifiquement vérifiables attestant l'existence du problème.

- Définir précisément l'objectif d'intérêt général ou le droit d'autrui que la mesure cherche à réaliser/respecter.
- Veiller à ce que la finalité du traitement des données à caractère personnel réponde effectivement à un objectif d'intérêt général reconnu par l'Union ou au besoin de protection des droits et libertés d'autrui.
- Expliquer l'importance de l'objectif à réaliser et à quel point cet objectif est indispensable au bon fonctionnement de la société.

Conclusions

- ✓ **Si le problème à résoudre n'est pas suffisamment décrit**, il doit être mieux expliqué et développé. Dans le cas contraire, l'évaluation de la nécessité de la mesure sera impossible.
- ✓ **Si le problème n'est pas étayé par des éléments de preuve suffisants**, d'autres éléments de preuve doivent être recherchés.
- ✓ **Si la mesure ne répond pas effectivement à un objectif d'intérêt général reconnu par l'Union ou au besoin de protection des droits et libertés d'autrui**, alors la mesure ne doit pas être proposée.
- ✓ **Si la mesure permet de réaliser un tel objectif**, étayé par des éléments de preuve suffisants, alors la nécessité de la mesure peut être évaluée conformément à l'étape 4.

Exemples pertinents

EXEMPLE 7: *Digital Rights Ireland* (CJUE, affaires jointes C-293/12 et C-594/12)

Aux fins d'évaluer la légalité de la directive sur la conservation des données (directive 2006/24/CE), la CJUE a tenu compte des conclusions du Conseil «Justice et affaires intérieures» du 19 décembre 2002 qui indiquent que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée (point 43). La Cour a également reconnu qu'il ressort de sa jurisprudence que la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationale constitue un objectif d'intérêt général. Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (article 42). En conséquence, la Cour a jugé que «*la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24/CE, répond effectivement à un objectif d'intérêt général*» (point 44).

EXEMPLE 8: *Promusicae* (CJUE, affaire C-275/06)

La CJUE a jugé que la protection du droit de propriété intellectuelle constituait un objectif légitime au regard du traitement des données relatives aux communications (adresses IP), comme le prévoit l'article 13 de la directive 95/46/CE qui énonce les objectifs légitimes pour imposer des limitations au droit au respect de la vie privée en ce qui concerne le traitement des données à caractère personnel (point 26).

EXEMPLE 9: Avis du CEPD du 9 octobre 2012 *sur la modification de la proposition de la Commission COM(2011) 628 final/2 pour un règlement du Parlement européen et du Conseil relatif au financement, à la gestion et au suivi de la politique agricole commune* [réglementation adoptée en vue de se conformer à l'arrêt *Schecke* sur la publication des données à caractère personnel relatives aux bénéficiaires d'aides dans le cadre de la politique agricole commune – à présent le règlement (UE) nº 1306/2013, en particulier les articles 111 à 113 et les considérants 73 à 87]

Si le CEPD a reconnu, comme dans l'arrêt *Schecke* (points 65, 68, 69, 75), que la transparence et le contrôle public constituaient des objectifs d'intérêt général, le problème de la réduction du nombre de contrôles spécifiques et de contrôles sur place par les autorités en raison des contraintes économiques ne pouvait s'inscrire dans le cadre de l'objectif susmentionné: «*La transparence et le contrôle public sont des objectifs légitimes en tant que tels [...] et ne peuvent pas être présentés comme des substituts aux contrôles spécifiques et aux contrôles sur place par les autorités compétentes [...]*.» (point 17).

EXEMPLE 10: Avis 3/2016 du CEPD *sur les échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS)*

Le CEPD a conclu que la proposition de la Commission relative au système ECRIS visant à faciliter l'accès aux informations sur les condamnations de ressortissants de pays tiers relevait du domaine de la lutte contre le terrorisme et contre la grande criminalité en vue d'assurer la sécurité publique, cette lutte étant reconnue comme un objectif d'intérêt général en droit de l'Union. «*Dès lors, les mesures proposées répondent à un objectif d'intérêt général et peuvent être justifiées, dans le respect du principe de proportionnalité*» (point 9).

Étape 4: Choix de l'option efficace et la moins intrusive

Dans la section II.2, il a été souligné qu'une mesure *pertinente* ne signifiait pas qu'elle était *efficace*. Même si elle est pertinente, la mesure choisie doit également être efficace et moins intrusive que les autres options permettant d'atteindre le même objectif.

Une mesure pertinente doit permettre de réaliser l'objectif poursuivi.

- Il doit exister **un lien logique entre la limitation et** les objectifs légitimes définis.
- L'objectif poursuivi doit être réalisé en conséquence directe de l'application de la mesure.
- Une mesure pertinente ne doit toutefois pas s'attaquer à tous les aspects particuliers du problème[53].

Orientations générales sur l'efficacité et le degré d'intrusion

- ✓ **La mesure doit être véritablement efficace**,c'est-à-dire essentielle à la réalisation de l'objectif d'intérêt général poursuivi.

- Les mesures qui «pourraient s'avérer utiles» aux fins d'un objectif donné ne sont pas toutes «souhaitables ou ne sauraient être toutes considérées comme une mesure nécessaire dans une société démocratique»[54]. Il ne suffit pas que la mesure soit simplement commode ou rentable[55].

- Les catégories choisies de personnes concernées, les catégories de données à caractère personnel collectées et traitées, la période de conservation des données, etc., doivent contribuer efficacement à la réalisation de l'objectif poursuivi.

- Si la mesure proposée prévoit le traitement de **données sensibles**, une plus grande rigueur doit être de mise lors de l'évaluation de l'efficacité.

    - Les données sensibles comprennent les données révélant l'origine ethnique ou raciale, les opinions politiques, les convictions religieuses ou similaires, l'état de santé, etc. Les données relatives aux infractions et aux condamnations pénales possèdent un statut similaire[56]. Les données génétiques et biométriques sont reconnues comme des données sensibles par les nouveaux instruments juridiques sur la protection des données à caractère personnel[57]. Le groupe de travail «Article 29» avait toutefois déjà souligné à plusieurs reprises le «caractère sensible» de ces données[58].

    - D'autres catégories de données, bien qu'elles ne soient pas strictement classées comme sensibles, peuvent présenter, dans certains contextes, un risque plus élevé pour l'individu et déclencher l'application de critères allant au-delà de ce qui est strictement nécessaire. C'est le cas, par exemple, des identifiants uniques, comme les numéros nationaux d'identification ou les données financières.

✓ La mesure envisagée doit être **la moins intrusive au regard des droits en jeu**.

- D'autres mesures qui constituent une menace moindre au droit à la protection des données à caractère personnel et au droit au respect de la vie privée doivent être recensées.

- Ces mesures peuvent aussi être des combinaisons de mesures.

- Elles doivent non seulement être réelles, mais également présenter une efficacité suffisante et comparable pour résoudre le problème en question[59].

- L'imposition d'une limitation à une partie de la population/zone géographique est moins intrusive que l'imposition à l'ensemble de la population/zone géographique; une limitation à court terme est moins intrusive qu'une limitation à long terme; le traitement d'une catégorie de données est en général moins intrusif que le traitement de plusieurs catégories de données[60].

- Les économies de ressources ne doivent pas avoir une incidence sur les mesures de rechange. Cet aspect doit être évalué dans le cadre de l'examen

de la proportionnalité, étant donné qu'il requiert de trouver un juste équilibre avec les autres objectifs d'intérêt public (voir section II.2).

- ✓ **Chaque aspect particulier** de la mesure doit être soumis au critère de la stricte nécessité.
    - Certaines dispositions spécifiques, comme le traitement d'une catégorie de données à caractère personnel, les catégories de personnes concernées ou la durée de la conservation des données, peuvent se révéler nécessaires, contrairement à d'autres. L'évaluation d'une mesure dépend des «règles claires et précises régissant la portée et l'application de la mesure»[61]. Comme il a été mentionné à la section II.1, des règles claires et précises sont également importantes en vue de se conformer à la plupart des autres critères énoncés à l'article 52, paragraphe 1, de la charte.
    - Si la mesure prévoit l'accès des autorités aux données, elle doit établir des **critères objectifs** limitant en particulier le nombre de personnes autorisées à accéder aux données et à les utiliser à ce qui est strictement nécessaire[62].
    - La mesure doit opérer une **différenciation**, une **limitation** et des **exceptions**[63] pour les personnes dont les informations sont utilisées en fonction de l'objectif poursuivi.
    - S'agissant de la **période de conservation** des données, la mesure doit établir **une distinction entre les catégories de données** en fonction de leur **utilité effective** aux fins des objectifs poursuivis et doit être fondée sur des critères objectifs pour déterminer la durée de la période de conservation[64].
    - La limitation du **droit à l'information** au sujet du traitement des données à caractère personnel doit également être nécessaire aux fins de l'objectif poursuivi par la mesure proposée. Par exemple, l'objectif des mesures de surveillance secrète peut justifier la restriction de la notification aux personnes concernées. «*Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la [mesure].*»[65]
- ✓ **Les raisons justifiant la nécessité de la mesure** doivent être détaillées:
    - Raisons pour lesquelles les mesures actuelles sont insuffisantes pour résoudre le problème.
    - Raisons pour lesquelles les autres mesures moins intrusives sont insuffisantes pour résoudre le problème.
    - Raisons pour lesquelles la mesure proposée peut résoudre le problème **plus efficacement que les autres mesures**.
    - Des éléments de preuve objectifs pour l'ensemble des raisons susmentionnées doivent être fournis. Ils peuvent consister en des faits ou des données statistiques et doivent non seulement permettre une

vérification scientifique, mais également convaincre de la nécessité de la mesure proposée.

- Le critère de la nécessité ne doit pas être appliqué à chaque État membre individuellement, bien qu'il soit utile aux fins de l'analyse d'impact qui porte sur la valeur ajoutée de l'intervention de l'Union[66].

Procédure à suivre

- ✓ **Expliquer dans quelle mesure et pour quelles raisons la mesure est essentielle pour résoudre le problème:**
  - Raisons pour lesquelles les mesures actuelles sont insuffisantes pour résoudre le problème.
  - Raisons pour lesquelles la mesure permet de réaliser l'objectif poursuivi et de quelle manière.
- ✓ **Déterminer si d'autres mesures moins intrusives pourraient être aussi efficaces pour atteindre l'objectif poursuivi.**
- ✓ Fournir des éléments de preuves scientifiquement vérifiables qui peuvent réellement étayer l'affirmation selon laquelle les mesures actuelles et d'autres mesures moins intrusives ne permettent pas de résoudre efficacement le problème.

Conclusions

- ✓ **Envisager une mise en œuvre adéquate des mesures actuelles plutôt que de nouvelles mesures intrusives.**
- ✓ **Envisager une autre mesure qui soit aussi efficace, mais qui ait moins d'incidence sur la protection des données à caractère personnel ou le droit au respect de la vie privée.** La question d'une hausse des coûts peut être prise en considération dans le cadre de l'examen de la proportionnalité.
- ✓ **Uniquement si les mesures actuelles ou des mesures moins intrusives ne sont pas disponibles selon** une analyse fondée sur des données probantes, et uniquement si une telle analyse montre que la mesure envisagée est **essentielle et limitée à ce qui est absolument nécessaire** pour réaliser l'objectif d'intérêt général, alors cette mesure doit satisfaire au critère de la proportionnalité (voir section II.2).

Exemples pertinents

EXEMPLE 11: *Österreichischer Rundfunk e.a.* (CJUE, affaires jointes C-465/00, C-138/01 et C-139/01)

Pour déterminer si une large divulgation des noms et des salaires des employés de différents organismes publics qui faisaient l'objet d'un contrôle de la Cour des comptes respectait le droit à la vie privée, la CJUE a invité les juridictions nationales à examiner si l'objectif poursuivi par une telle divulgation «n'aurait pu être atteint de manière aussi *efficace par la transmission des informations nominatives aux seules instances de contrôle*» (point 88).

EXEMPLE 12: *Schecke* (CJUE, affaires jointes C-92/09 et C-93/09)

Lors de l'examen de la nécessité de la publication des données à caractère personnel de tous les bénéficiaires de fonds publics, la Cour a souligné que le législateur n'avait pas pris en considération d'autres mesures moins intrusives, telles que la limitation de la publication de données nominatives relatives auxdits bénéficiaires en fonction des périodes pendant lesquelles ils ont perçu des aides, de la fréquence ou encore du type et du montant de celles-ci. La Cour a également souligné qu'une approche moins intrusive pourrait être adoptée par une combinaison de ces mesures: «*Une publication nominative ainsi limitée pourrait, le cas échéant, être accompagnée d'explications pertinentes concernant les autres personnes physiques bénéficiaires d'aides [du FEAGA et du Feader] et les montants perçus par ces dernières.*» La Cour a conclu: «*Eu égard au fait que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt Satakunnan Markkinapörssi et Satamedia, point 56) et que des mesures portant des atteintes moins importantes pour les personnes physiques audit droit fondamental sont concevables tout en contribuant de manière efficace aux objectifs de la réglementation de l'Union en cause [...]*.» (points 81, 82, 83 et 86).

EXEMPLE 13: *Tele2 Sverige AB* (CJUE, affaires jointes C-203/15 et C-698/15)

Dans ses conclusions, l'avocat général a réaffirmé: «*Eu égard à l'exigence de stricte nécessité, il est impératif que ces juridictions ne se contentent pas de vérifier la simple utilité d'une obligation générale de conservation de données, mais vérifient strictement qu'aucune autre mesure ou combinaison de mesures, et notamment une obligation ciblée de conservation de données accompagnée d'autres outils d'investigation, ne peut offrir la même efficacité dans la lutte contre les infractions graves. Je souligne à cet égard que plusieurs études portées à l'attention de la Cour remettent en cause la nécessité de ce type d'obligation aux fins de la lutte contre les infractions graves.*» Ces autres mesures doivent être efficaces par rapport à l'objectif poursuivi. «*De telles obligations [de conservation des données] peuvent en effet avoir une étendue matérielle plus ou moins grande, en fonction des utilisateurs, des zones géographiques et des moyens de communication visés.*» (points 209 et 211).

La CJUE a jugé qu'une conservation ciblée pourrait être justifiée à condition qu'elle n'excède pas les limites du strictement nécessaire aux fins de la lutte contre les infractions graves: «*[...] la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, [doit être] limitée au strict nécessaire.*» Par ailleurs, «*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».* La Cour a également considéré que l'accès des autorités compétentes à ces données devait se fonder sur des critères objectifs et ne saurait, en principe, être accordé qu'aux données de personnes soupçonnées. Toutefois, «*[...] dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un*

cas concret, apporter une contribution effective à la lutte contre de telles activités» (points 102, 103, 108, 111, 115 et 119).

EXEMPLE 14: Avis 1/15 de l'avocat général (demande d'avis présentée par le Parlement européen) *sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers*

En ce qui concerne la stricte nécessité de la mesure, l'avocat général a souligné que les termes de l'accord envisagé «*doivent aussi consister dans les mesures les moins attentatoires aux droits reconnus par les articles 7 et 8 de la charte, tout en contribuant de manière efficace à l'objectif de sécurité publique poursuivi par l'accord envisagé. [...] Il faut encore que ces mesures alternatives soient suffisamment efficaces, c'est-à-dire qu'elles présentent [...] une efficacité comparable à celles prévues par l'accord envisagé, en vue de réaliser l'objectif de sécurité publique poursuivi par celui-ci».* En ce qui concerne ce critère de la nécessité, l'avocat général traite différents aspects de la mesure, tels que: «*[...] les catégories de données figurant à l'annexe de l'accord envisagé devraient être rédigées de manière plus concise et précise, sans qu'aucune marge d'appréciation puisse être laissée soit aux transporteurs aériens, soit aux autorités canadiennes compétentes quant à la portée concrète de ces catégories.*» *«Ce constat laisse penser, à défaut d'explication plus étayée dans l'accord envisagé quant à la stricte nécessité de traiter les données sensibles, que l'objectif de lutte contre le terrorisme et contre la criminalité internationale grave peut être réalisé de manière tout aussi efficace sans que de telles données soient même transférées au Canada.» «[...] pour limiter au strict nécessaire les infractions susceptibles d'autoriser le traitement de données PNR et assurer la sécurité juridique des passagers dont les données sont transmises aux autorités canadiennes, [...] les infractions [...] devraient être limitativement énumérées [...].*» S'agissant de la durée de conservation, l'avocat général a indiqué que «*l'accord envisagé n'indique pas les raisons objectives qui ont conduit les parties contractantes à porter la durée de conservation des données PNR à cinq ans maximum.*» (points 205, 220, 222, 235, 261 et 267).

EXEMPLE 15: Avis 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*, 25 mars 2011

Le CEPD a constaté que l'analyse d'impact de la directive proposée comprenait d'abondantes explications et statistiques visant à justifier la mesure, mais que ces éléments n'étaient pas convaincants. À titre d'exemple, la description de la menace du terrorisme et des formes graves de criminalité dans l'analyse d'impact ainsi que dans l'exposé des motifs de la proposition citait le nombre de 14 000 infractions pénales par tranche de 100 000 habitants dans les États membres en 2007. Si ce chiffre pouvait paraître impressionnant, il concernait des types de criminalité non différenciés et ne pouvait en aucune façon contribuer à justifier une mesure qui ne ciblait et ne combattait qu'un type limité de criminalité grave et transnationale et de terrorisme. Autre exemple, le fait de citer un rapport sur les «problèmes» de drogue sans lier les statistiques au type de trafic de stupéfiants concerné par la proposition ne constituait pas selon le CEPD une référence valable (point 11). Le CEPD a conclu que les documents de référence n'étaient pas suffisamment pertinents et précis pour démontrer la nécessité de l'instrument (point 12).

EXEMPLE 16: Avis 7/2010 du groupe de travail «Article 29» *sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers*, 12 novembre 2010

S'agissant de l'évaluation de la nécessité des transferts des données des dossiers passagers aux pays tiers, le groupe de travail «Article 29» a conseillé à la Commission d'«*évaluer la possibilité de répondre aux demandes de données passagers formulées par les pays tiers grâce à ces systèmes et mécanismes existants, avant de conclure de nouveaux accords*». Le groupe de travail a également souligné qu'«*[i]l faut sérieusement envisager des solutions de remplacement avant de mettre en place un tel système, eu égard à la nature intrusive des décisions prises, du moins pour une large part, de manière automatisée sur la base de pratiques courantes, et en raison de la difficulté, pour les citoyens, de s'opposer à de telles décisions*» (page 5).

EXEMPLE 17: Avis 3/2016 du CEPD *sur les échanges d'informations relatives aux ressortissants de pays tiers dans le cadre du système européen d'information sur les casiers judiciaires (ECRIS)*, 13 avril 2016

La proposition législative à l'étude prévoit l'obligation pour les États membres d'inclure les données biométriques (empreintes digitales) de l'ensemble des ressortissants de pays tiers ayant fait l'objet d'une condamnation dans le système ECRIS, faisant valoir cette nécessité aux fins d'identification. Le CEPD a demandé que d'autres éléments de preuve soient fournis afin de démontrer la nécessité de conserver les empreintes digitales. «*Dès lors, on ne saurait considérer qu'il n'existe pas d'autre moyen, pour assurer l'identification des personnes, que l'utilisation des empreintes digitales et, en conséquence, la nécessité de l'obligation d'utilisation des empreintes digitales pour les RPT dans l'ECRIS n'a pas été démontrée.*» (point 15).

EXEMPLE 18: Avis 5/2015 du CEPD *sur la proposition de directive relative à l'utilisation des données des dossiers passagers*

Le CEPD a souligné: «*D'après les éléments disponibles, les toutes dernières versions de la proposition n'attestent pas de la réalisation d'une véritable évaluation, conforme à la jurisprudence de la CJCE, des lacunes persistant dans la lutte contre le terrorisme ainsi que des moyens possibles d'y remédier à l'aide des instruments dont disposent actuellement les États membres. Si cette évaluation devrait également aborder les nouvelles méthodes d'enquête destinées à surveiller plus efficacement les suspects connus des autorités policières et judiciaires, divers événements survenus ces derniers temps au sein de l'UE mettent en évidence des lacunes en matière de renseignement ne concernant pas les passagers du transport aérien et le fait qu'il serait, dans certains cas, plus efficace de concentrer les ressources sur les suspects connus, et d'intensifier les efforts déployés à leur égard, que de réaliser le profilage par défaut de millions de voyageurs.*» (point 14).

EXEMPLE 19: Lettre du groupe de travail «Article 29» à la commission LIBE *sur le projet PNR européen*, 19 mars 2015

Le groupe de travail «Article 29» a souligné que la nécessité d'un système de PNR européen devait être justifiée, c'est-à-dire qu'il convient de clarifier pourquoi les instruments existants (SIS, API) ne sont pas suffisants, d'expliquer en quoi des alternatives moins intrusives ne permettraient pas de réaliser l'objectif et de préciser en quoi le système de PNR européen est la solution pour réaliser l'objectif, par opposition aux mesures moins intrusives. Les explications devaient être étayées par des éléments de preuve, éventuellement des statistiques, ou par des études de l'Union ou des États membres.

EXEMPLE 20: Avis 7/2016 du CEPD *sur le premier paquet de mesures pour une réforme du régime d'asile européen commun (Eurodac, EASO et règlement de Dublin)*

Le CEPD a souligné que la nécessité d'ajouter une deuxième catégorie de données biométriques, c'est-à-dire des images faciales, dans une base de données de grande envergure devait être fondée sur «*[...] une évaluation [...] sur la base d'une étude cohérente ou d'une approche fondée sur des données probantes*».
En ce qui concernait la période de conservation, le CEPD a souligné que l'augmentation de la période de conservation à cinq ans afin de l'aligner sur ce que les autres instruments prévoyaient «*n'est pas pertinente en tant que telle, dans la mesure où lesdits instruments peuvent avoir des finalités différentes et où leur durée de conservation peut être justifiée par d'autres éléments*». Dans son avis, le CEPD a considéré que la durée de conservation de cinq ans n'était pas suffisamment justifiée et a recommandé de fournir davantage d'éléments justificatifs (points 22, 30 et 31).

Notes

[1] L'article 2 du traité sur l'Union européenne (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*». Par ailleurs, l'article 6, paragraphe 1, du TUE reconnaît les droits, les libertés et les principes énoncés dans la charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adoptée à Strasbourg le 12 décembre 2007, qui a la même valeur juridique que les traités. De même, l'article 6, paragraphe 3, du TUE établit 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*».

[2] Le 24 mai 2016, le CEPD a annoncé à la commission des libertés civiles du Parlement européen son intention de publier le présent guide.

[3] Voir outil#24 «Droits fondamentaux & droits de l'homme» de la boîte à outils pour une meilleure réglementation (http://ec.europa.eu/smart-regulation/guidelines/tool_24_fr.htm) et l'analyse plus approfondie fournie 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. Voir également Conseil, «Guidelines on methodological steps to be taken to check fundamental rights compatibility at the Council preparatory bodies», 5377/15, 20 janvier 2015. Ces documents sont de nature plus générale, bien que plusieurs exemples de jurisprudence figurant dans ces lignes directrices portent sur les droits reconnus dans les articles 7 et 8 de la charte, la CJUE ayant rendu des arrêts importants sur la limitation de ces droits.

[4] Pour un aperçu de la jurisprudence pertinente de la CJUE et de la CouEDH, voir «Manuel de droit européen en matière de protection des données», publié par l'Agence des droits fondamentaux de l'Union européenne en juin 2014. Voir également «Fiche thématique - Protection des données personnelles», publiée en novembre 2016 par l'unité de la Presse de la CouEDH, disponible à l'adresse suivante: http://www.echr.coe.int/Documents/FS_Data_FRA.pdf.

[5] Voir «Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights», disponible à l'adresse suivante:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Papers/16-06-16_Necessity_paper_for_consultation_EN.pdf.

[6] Dans les affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, l'avocat général a déclaré dans ses conclusions: «*Comme 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 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*», point 73. Cette approche est adoptée dans l'arrêt de la CJUE, points 48 à 50.

[7] En ce qui concerne la notion «prévue par la loi», les critères fixés par la CouEDH doivent être utilisés comme il est suggéré dans plusieurs conclusions d'avocats généraux de la CJUE; voir, par exemple, conclusions des avocats généraux dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, points 137 à 154, dans l'affaire C-70/10, *Scarlet Extended*, points 88 à 114, et dans l'affaire C-291/12, *Schwarz*, point 43. Cette approche est adoptée dans le considérant 41 du règlement général (UE) 2016/679 sur la protection des données.

[8] Alors que la jurisprudence n'est 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 empêcherait ainsi l'exercice du droit. Dans l'affaire *Schrems,* la CJUE a conclu qu'il était porté atteinte au contenu essentiel du droit à un recours effectif. «*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 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*» (point 95). En conséquence, elle n'a pas poursuivi l'examen visant à déterminer si une limitation était nécessaire, mais elle a déclaré invalide, également pour d'autres motifs, la décision de la Commission relative à la pertinence de la protection

assurée par les principes de la «sphère de sécurité». Dans l'affaire *Digital Right Ireland*, la CJUE a conclu que la conservation des données n'était pas de nature à porter atteinte au contenu essentiel du droit au respect à la vie privée, étant donné que la directive sur la conservation des données ne permettait pas de prendre connaissance du contenu des communications électroniques. 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, en raison du fait que 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 (points 39 et 40). Ce n'est qu'alors que la CJUE a examiné la nécessité de la mesure. 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*», voir affaire *Tele2 Sverige AB*, point 123.

[9] Dans l'arrêt *Szabo et Vissy c. Hongrie*, rendu le 12 janvier 2016, la CouEDH a conclu que la notion de «*personnes concernées identifiées […] comme une série de personnes*» pouvait couvrir toute personne sans que les autorités aient l'obligation de démontrer la relation entre les personnes concernées et la prévention d'une attaque terroriste. Une telle mesure ne satisfait pas aux exigences de prévisibilité et de nécessité (paragraphes 58, 62, 66 et 67).

[10] Voir article 5, paragraphe 4, du traité établissant l'Union européenne.

[11] Affaire C-62/14, *Gauweiler (OMT)*, point 67.

[12] 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 Eifert*, 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).

[13] Voir, par exemple, affaire C-83/14 *Razpredelenie Bulgaria Ad,* point 123. La Cour déclare que «*[…] à supposer qu'aucune autre mesure aussi efficace que la pratique litigieuse ne puisse être identifiée, la juridiction de renvoi devra encore vérifier si les inconvénients causés par la pratique litigieuse ne sont pas démesurés par rapport aux objectifs poursuivis et si cette pratique ne porte pas une atteinte excessive aux intérêts légitimes des personnes habitant les quartiers concernés*». Voir, également, conclusions de l'avocat général dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, points 132, 172, 247 et 248, dans lesquelles il a déclaré que, dans l'affaire Digital Rights Ireland, la CJUE n'a pas procédé à l'examen de la proportionnalité «*étant donné que le régime établi par la directive 2006/24/CE excédait les limites de ce qui est strictement nécessaire aux fins de la lutte contre les infractions graves*». Il a ensuite indiqué que l'«*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/CE, de l'article 52, paragraphe 1, de la charte 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*». Il a également souligné que l'exigence de proportionnalité dans le cas particulier de la conservation d'un tel volume 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*». Dans son arrêt, la Cour expose, aux points 102 et 103, son analyse en tenant plutôt compte de la proportionnalité au moment de déterminer si la lutte contre la criminalité, voire la criminalité grave, justifie une conservation généralisée et indifférenciée des données de communications électroniques. La Cour affirme que «*[…] si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul 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*». Elle ajoute également que seule la lutte contre la criminalité grave pourrait justifier une conservation ciblée et un accès aux données de communications électroniques. «*Eu 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.*» «*En outre, dès lors que l'objectif poursuivi par cette réglementation doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, il s'ensuit que, en matière de prévention, de recherche, de détection et de*

poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données conservées.»

[14] Voir article 6, paragraphe 1, point c), et article 7 de la directive 95/46/CE, article 4, paragraphe 1, point c), et article 5 du règlement (CE) nº 45/2001, article 5, paragraphe 1, point c), et article 6, paragraphe 1, du règlement (UE) 2016/679, ainsi que considérant 49, qui met l'accent sur le critère de la stricte nécessité en ce qui concerne le traitement des données à caractère personnel aux fins de garantir la sécurité du réseau et des informations des systèmes du responsable du traitement, et article 8, paragraphe 1, de la directive (UE) 2016/680.

Dans les lignes directrices adressées aux institutions de l'Union en vue de déterminer si des mesures de vidéosurveillance sont nécessaires conformément au règlement (CE) nº 45/2001, le CEPD a souligné qu'«*[i]l ne faut pas installer de système de vidéosurveillance dans les cas où ce système ne permettra pas d'atteindre l'objectif attendu, par exemple s'il donne uniquement l'illusion d'une meilleure sécurité*» (chapitre 5.4) «*et si des alternatives adéquates sont disponibles*». «*Une alternative peut être considérée comme adéquate sauf si elle n'est pas réalisable, si elle est nettement moins efficace que la vidéosurveillance [...]*» «*Le simple fait que la technologie soit disponible à un prix relativement peu élevé ne suffit pas à justifier l'utilisation de la vidéosurveillance.*» (chapitre 5.5). Ce n'est qu'alors qu'il est déterminé si la mesure est proportionnelle. «*Enfin, même si une institution arrive à la conclusion qu'il existe un besoin réel d'utiliser la vidéosurveillance et qu'il n'existe pas d'autre méthode moins intrusive, elle ne doit avoir recours à cette technologie que si les effets négatifs de la vidéosurveillance sont compensés par ses avantages.*» (chapitre 5.6). Voir «Lignes directrices du CEPD en matière de vidéosurveillance», Bruxelles, 17 mars 2010, disponible à l'adresse suivante:https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_FR.pdf. Dans le cadre d'une notification pour contrôle préalable, en vertu de l'article 27 du règlement (CE) nº 45/2001, d'une mesure qui proposait l'utilisation des empreintes digitales pour contrôler le temps de travail, le CEPD a souligné qu'un tel traitement n'était pas nécessaire. «*Le CEPD signale que l'utilisation de systèmes fondés sur les empreintes digitales pour contrôler le temps de travail des membres du personnel n'est pas jugée nécessaire et n'est dès lors pas légitime, en vertu dudit article 5 [règlement (CE) nº 45/2001]. Compte tenu de la nécessité du traitement des données à caractère personnel aux fins de l'objectif poursuivi, le responsable du traitement est tenu de déterminer si l'objectif du traitement pourrait être réalisé par des moyens moins intrusifs. En effet, au lieu d'opter pour un système utilisant les données biométriques, d'autres systèmes auraient dû être pris en considération par l'[organe de l'Union] dans ce contexte, tels que: la signature de fiches de présence ou l'enregistrement des heures au moyen de badges magnétiques.*» (chapitre 3), voir lettre du CEDP ayant pour objet: «Prior checking notification concerning 'Processing of leave and flexitime'», 13 octobre 2014, disponible à l'adresse suivante: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Letters/2014/14-10-13_Letter_Mr_Mifsud_EBA_EN.pdf.

[15] Dans les affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, la Cour a tout d'abord indiqué que le principe de proportionnalité consistait à juger du caractère approprié et nécessaire d'une 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), avant de conclure que les limitations n'étaient pas proportionnées (point 69). De même, dans l'affaire C-362/14, *Schrems*, 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).

[16] Par exemple, dans les affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, la Cour expose aux points 102 et 103 son analyse en tenant compte de la proportionnalité au sens strict au moment de déterminer si la lutte contre la criminalité, voire la criminalité grave, justifie une conservation généralisée et indifférenciée des données de communications électroniques. La Cour affirme que «*[...] si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul 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*». Elle ajoute également que seule la lutte contre la criminalité grave pourrait justifier une conservation ciblée et un accès aux données de communications électroniques. «*Eu 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.» «*En outre, dès lors que l'objectif poursuivi par cette réglementation doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, il s'ensuit que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données conservées.*» Ce n'est qu'ensuite qu'elle procède à l'analyse des exigences de nécessité d'une conservation ciblée des données de communications (point 108).

[17] Voir également avis 4/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel, page 7.

[18] Les récents arrêts historiques de la CJUE dans le domaine de la protection des données, en particulier les arrêts *Digital Rights Ireland* et *Schrems*, illustrent ces propos.

[19]Voir CJUE, affaire C-617/10, *Åkerberg Fransson*, point 44; affaire C-398/13 P, *Inuit Tapiriit Kanatami e.a./Commission*, point 45; affaire C-601/15 PPU *J. N./Staatssecretaris van Veiligheid en Justitie*, point 45, et affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, points 127 à 129.

[20] Voir CJUE, affaire C-199/11, *Otis e.a.*, point 47; affaire C-398/13 P, *Inuit Tapiriit Kanatami e.a./Commission*, point 46, et affaire C-601/15 PPU, *J. N./Staatssecretaris van Veiligheid en Justitie*, point 46.

[21] Voir affaire C-601/15 PPU, *J. N./Staatssecretaris van Veiligheid en Justitie*, point 77.

[22] Voir explication ad article 52 de la charte.

[23] Voir H. Kranenborg, article 8, p. 235, S. Peers et J. Kenner, *EU Charter of Fundamental Rights*, 2014 et S. Peers, article 52, p. 1 515 et. seq., ibid.

[24] Voir, par exemple, CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, point 59; affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 35; affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, points 119 et 120, et CouEDH; affaire *Zakharov c. Russie*, 4 décembre 2015, et affaire *Szabo et Vissy c. Hongrie*, 12 janvier 2016, paragraphe 23.

[25] Article 8, paragraphe 2, de la CEDH: *«Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui,* ***dans une société démocratique, est nécessaire*** *à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*» En ce qui concerne la charte, voir article 52, paragraphe 1 – «*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.*»

[26] Pour une analyse détaillée de la jurisprudence de la CouEDH sur l'application des exigences énoncées à l'article 8, paragraphe 2, de la convention, voir avis 1/2014 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.

[27] CouEDH, *Szabo et Vissy c. Hongrie*, 12 janvier 2016, paragraphe 73.

[28] Voir CJUE, affaire C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy*, point 56; affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, point 77; affaire C-473/12, *IPI*, point 39; affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger e.a.*, point 52; affaire C-212/13, *Rynes*, point 28; affaire C-362/14, *Schrems*, point 92; affaires jointes C-203/15 et C-698/15, *Tele2 Sverige AB*, point 96, et avis 1/15 de l'avocat général (demande d'avis présentée par le Parlement européen) sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, point 226.

[29] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016.

[30] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, points 47 et 48.

[31] CEPD, plaidoirie orale dans l'affaire portant sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, disponible à l'adresse suivante:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2016/16-04-05_Pleading_Canada_PNR2_EN.pdf. Dans son avis 1/15 (demande d'avis présentée par le Parlement européen) sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, l'avocat général indique que le contrôle strict du pouvoir d'appréciation du législateur repose sur le rôle important que joue le traitement des données à caractère personnel dans la société et sur la gravité de la limitation que la mesure en question peut causer (point 201). Voir également CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 47.

[32] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, points 34 à 36; voir également affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, point 58.

[33] Voir, par exemple, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, point 55, et affaires jointes C-468/10 et C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD)/Administración del Estado*, point 41. La CJUE n'a jugé que dans une seule affaire qu'il n'y avait pas de limitation au droit à la vie privée lorsque les données à caractère personnel liées aux salaires étaient traitées par les employeurs aux mêmes fins qu'à l'origine; voir CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof e.a./Österreichischer Rundfunk*, point 74.

[34] CJUE; affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof e.a./Österreichischer Rundfunk*, point 75, et affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 33.

[35] CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Rechnungshof e.a./Österreichischer Rundfunk*, point 75; affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 33. CouEDH, *S. et Marper c. Royaume-Uni*, 4 décembre 2008, paragraphe 67. La Cour a indiqué: «*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 (voir, mutatis mutandis, Friedl, précité, avis de la Commission, §§ 49-51, et Peck c. Royaume-Uni, précité, § 59).*»

[36] Par ailleurs, comme la CJUE l'a indiqué, la notion de nécessité est autonome dans le droit dérivé de l'Union. En ce qui concerne la signification autonome de la notion de nécessité telle qu'elle résulte de l'article 7, point e), de la directive 95/46/CE, voir CJUE, affaire C-524/06, *Huber/Bundesrepublik Deutschland*, point 52.

[37] Voir directive 95/46/CE, article 2, point a).

[38] Voir avis 4/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel, disponible à l'adresse suivante:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf.

[39] CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Österreichischer Rundfunk e.a.*, point 75, et affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 33.

[40] CouEDH, affaire *Leander c. Suède*, 26 mars 1987, paragraphe 48.

[41] CouEDH, affaire *Amman c. Suisse*, 16 février 2000, paragraphes 65, 69 et 80.

[42] En ce qui concerne l'article 8 de la CEDH, voir affaire *Leander c. Suède*, 26 mars 1987, paragraphe 48; affaire *Rotaru c. Roumanie*, 4 mai 2000, paragraphe 46; et affaire *Weber et Saravia c. Allemagne*, 29 juin 2006, paragraphe 79, CouEDH 2006-XI. En ce qui concerne l'article 7 de la charte, voir CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 35.

[43] CouEDH, affaire *Leander c. Suède*, 26 mars 1987, paragraphe 48; affaire *Rotaru c. Roumanie*, 4 mai 2000, paragraphe 46.

[44] CJUE, affaire C-362/14, *Schrems*, point 97.

[45] CJUE, affaire C-524/06, *Huber*, points 75, 79, 80 et 81.

[46] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 28; affaires jointes C-203/15 et C-698/15,*Tele2 Sverige AB,* point 92. Voir également C. Docksey, *Four Fundamental rights: finding the balance*, (2016) 6 International Data Privacy Law, p. 2.

[47] Avis 1/15 de l'avocat général (demande d'avis présentée par le Parlement européen) sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, points 274 à 281.

[48] Par exemple les articles 36 et 346 TFUE. En ce qui concerne les objectifs d'intérêt général, voir également explication ad article 52 de la charte.

[49] CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke*, points 65, 68, 69 et 75.

[50] CJUE, affaire C-275/06, *Productores de Música de España (Promusicae)/Telefónica de España SAU*, point 65; affaire C-70/10, *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, points 46, 49 et 53.

[51] CJUE, affaire C-145/09, *Tsakouridis*, sur la notion de «sécurité publique», points 43 et 44; affaire C-601/15 PPU, *J. N./Staatssecretaris voor Veiligheid en Justitie*, point 66.

[52] CEPD, avis 2/2016 sur la proposition de règlement relatif au corps européen de garde-frontières et de garde-côtes, point 8.

[53] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland,* points 49 et 50.

[54] Groupe de travail «Article 29», avis 9/2004 sur sur le projet de décision-cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques, WP 99, 9 novembre 2004.

[55] Groupe de travail «Article 29», avis 3/2012 sur l'évolution des technologies biométriques, WP 193, 27 avril 2012, p. 8.

[56] Voir article 8 de la directive 95/46/CE, articles 9 et 10 du règlement général (UE) 2016/679 sur la protection des données, et directive (UE) 2016/680.

[57] Article 9 du règlement (UE) 2016/679, article 10 de la directive (UE) 2016/680.

[58] Voir, par exemple, groupe de travail «Article 29», avis 3/2012 sur l'évolution des technologies biométriques, p. 4.

[59] Dans l'affaire C-291/12, *Schwarz*, la CJUE a jugé: «*Dans ces conditions, il y a lieu de constater qu'il n'a pas été porté à la connaissance de la Cour l'existence de mesures susceptibles de contribuer, de manière suffisamment efficace, au but tenant à la protection des passeports contre leur utilisation frauduleuse, tout en portant des atteintes moins importantes aux droits reconnus par les articles 7 et 8 de la charte que celles entraînées par la méthode fondée sur les empreintes digitales*», point 53; voir également avis 1/15 de l'avocat général (demande d'avis présentée par le Parlement européen) sur le projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, dans lequel il est mentionné que l'accord doit consister dans les mesures les moins attentatoires aux droits reconnus par les articles 7 et 8 de la charte et doit contribuer de manière efficace à la réalisation de l'objectif de sécurité publique, points 208 et 244.

[60] Il n'en va toutefois pas de même pour les identifiants d'application générale. Voir article 87 du règlement (UE) 2016/679.

[61] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 54, et jurisprudence citée de la CouEDH (affaire *Liberty e.a. c. Royaume-Uni*, paragraphes 62 et 63; affaire *Rotaru c. Roumanie*, paragraphes 57 à 59; et affaire *S. et Marper c. Royaume-Uni*, paragraphe 99).

[62] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland,* point 60; affaire C-362/14, *Schrems*, point 93.

[63] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland*, point 57; affaire C-362/14, *Schrems*, point 93.

[64] CJUE, affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland,* points 63 et 64.

[65] CouEDH, affaire *R. Zakharov c. Russie*, 4 décembre 2015, paragraphe 287. Voir également CouEDH, affaire *Szabo et Vissy c. Hongrie*, 12 janvier 2016, paragraphe 86.

[66] En ce qui concerne le principe de la subsidiarité, voir outil#3 «Base juridique, subsidiarité et proportionnalité» de la boîte à outils pour une meilleure réglementation (http://ec.europa.eu/smart-regulation/guidelines/tool_3_fr.htm).