GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

844/14/FR
WP 217

Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE

Adopté le 9 avril 2014

Table des matières

Résumé

Le présent avis analyse les critères légitimant le traitement des données énoncés à l'article 7 de la directive 95/46/CE. Il se concentre sur l'intérêt légitime poursuivi par le responsable du traitement et formule des orientations pour l'application de l'article 7, point f), dans le cadre juridique actuel, ainsi que des recommandations d'améliorations futures.

L'article 7, point f), est le dernier des six motifs qui rendent licite le traitement des données à caractère personnel. Dans les faits, il requiert la mise en balance de l'intérêt légitime poursuivi par le responsable du traitement, ou par les tiers auxquels les données sont communiquées, et des intérêts ou des droits fondamentaux de la personne concernée. Le résultat de cette mise en balance déterminera si l'article 7, point f), peut être invoqué pour justifier le traitement.

Le groupe de travail «Article 29» mesure toute l'importance et l'utilité du critère fixé par l'article 7, point f), qui, lorsque les circonstances s'y prêtent et moyennant des garanties adéquates, permet d'éviter un recours excessif à d'autres fondements juridiques. L'article 7, point f), ne saurait servir uniquement «en dernier ressort», dans les situations rares ou inattendues où l'on considère que les autres motifs légitimant le traitement ne s'appliquent pas. Il faut néanmoins éviter de s'y référer automatiquement ou d'en élargir indûment l'utilisation au prétexte qu'il semble moins contraignant que les autres motifs.

Une appréciation correcte de l'article 7, point f), ne se borne pas à une simple mise en balance consistant à peser deux «poids» aisément quantifiables et comparables. Le critère suppose un examen complet de plusieurs facteurs, de façon à garantir que les intérêts et les droits fondamentaux des personnes concernées sont dûment pris en considération. Il s'agit néanmoins d'un examen modulable qui peut varier en complexité et qui ne doit pas être inutilement contraignant. Les facteurs à prendre en considération dans cette mise en balance sont notamment:

- la nature et la source de l'intérêt légitime, et la question de savoir si le traitement des données est nécessaire à l'exercice d'un droit fondamental, est d'intérêt public à quelque autre égard ou bénéficie d'une reconnaissance dans la collectivité concernée;

- l'incidence sur les personnes concernées et leurs attentes raisonnables quant à ce qu'il adviendra de leurs données, ainsi que la nature des données et la façon dont elles sont traitées;

- les garanties supplémentaires qui pourraient limiter toute incidence injustifiée sur la personne concernée, comme la minimisation des données, les technologies renforçant la protection de la vie privée; une plus grande transparence, un droit général et inconditionnel de s'opposer au traitement et la portabilité des données.

Le groupe de travail «Article 29» recommande à l'avenir d'intégrer, dans la proposition de règlement, un considérant sur les facteurs-clés à examiner lors de l'application du critère de mise en balance. Il préconise aussi d'ajouter un considérant imposant au responsable du traitement, s'il y a lieu, de documenter son appréciation dans un souci de plus grande responsabilisation. Enfin, le groupe de travail «Article 29» serait favorable à l'ajout d'une disposition de fond exigeant des responsables du traitement qu'ils expliquent pourquoi ils considèrent que l'intérêt ou les droits et libertés fondamentaux des personnes concernées ne prévalent pas sur l'intérêt qu'ils poursuivent.

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

I. Introduction

Le présent avis analyse les critères légitimant le traitement des données énoncés à l'article 7 de la directive 95/46/CE[1] (ci-après la «directive»). Il se concentre, en particulier, sur l'intérêt légitime poursuivi par le responsable du traitement, au sens de l'article 7, point f).

Les critères énumérés à l'article 7 sont liés au principe plus large de «licéité» posé à l'article 6, paragraphe 1, point a), qui requiert que les données à caractère personnel soient traitées «loyalement et licitement».

L'article 7 n'autorise le traitement de données à caractère personnel que si au moins un des six fondements juridiques énumérés audit article s'applique. Concrètement, les données à caractère personnel seront traitées uniquement si: a) la personne concernée a indubitablement donné son consentement[2]; ou si – en résumé[3] – le traitement est nécessaire:

b) à l'exécution d'un contrat conclu avec la personne concernée;
c) au respect d'une obligation légale imposée au responsable du traitement;
d) à la sauvegarde de l'intérêt vital de la personne concernée;
e) à l'exécution d'une mission d'intérêt public; ou
f) à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, sous réserve du respect d'un critère supplémentaire de mise en balance avec les droits et l'intérêt de la personne concernée.

Ce dernier motif permet le traitement «nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou[4] les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1». Autrement dit, l'article 7, point f), autorise le traitement, sous réserve d'une mise en balance qui compare l'intérêt légitime poursuivi par le responsable du traitement – ou

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, 23.11.1995, p. 31).
[2] Voir l'avis 15/2011 du groupe de travail «Article 29» sur la protection des données concernant la définition du consentement, adopté le 13.7.2011 (WP 187).
[3] Ces dispositions sont examinées plus en détail à un stade ultérieur.
[4] *[Sans objet dans la version française, concerne une faute de frappe dans la version originale anglaise – voir le point III.3.2.]*

par le ou les tiers auxquels les données sont communiquées – avec l'intérêt ou les droits fondamentaux des personnes concernées[5].

Nécessité d'une approche plus cohérente et harmonisée en Europe

Il ressort des études réalisées par la Commission dans le cadre de la révision de la directive[6], ainsi que de la coopération et des échanges de vues entre les autorités nationales chargées de la protection des données, que l'absence d'une interprétation harmonisée de l'article 7, point f), de la directive a conduit à des applications divergentes dans les États membres. Notamment, bien que plusieurs États membres imposent une véritable mise en balance, l'article 7, point f), est parfois perçu à tort comme une «porte ouverte» légitimant tout traitement de données qui ne cadre avec aucun autre fondement juridique.

L'absence d'approche cohérente peut entraîner un manque de sécurité juridique et de prévisibilité, affaiblir la position des personnes concernées et aussi imposer des contraintes réglementaires inutiles aux entreprises et à d'autres organisations exerçant des activités transfrontières. De telles incohérences ont déjà donné lieu à des litiges portés devant la Cour de justice de l'Union européenne[7].

Il est donc particulièrement opportun, alors que le travail d'élaboration d'un nouveau règlement général sur la protection des données se poursuit, de veiller à ce que le sixième motif justifiant le traitement («l'intérêt légitime») et sa relation avec les autres motifs soient mieux compris. En particulier, dès lors que les droits fondamentaux des personnes concernées sont en jeu, il convient de prendre dûment en considération le respect de ces droits lors de l'application de chacun des six motifs, sans discrimination. L'article 7, point f), ne doit pas devenir un moyen commode d'échapper à l'obligation de se conformer au droit applicable en matière de protection des données.

C'est pourquoi, dans le cadre de son programme de travail 2012-2013, le groupe de travail «Article 29» sur la protection des données (ci-après le «groupe de travail») a décidé d'examiner attentivement la question et s'est engagé – en application de son programme de travail[8] – à rédiger le présent avis.

---

[5] La référence à l'article 1er, paragraphe 1, ne doit pas être interprétée comme une limitation de la portée de l'intérêt et des droits et libertés fondamentaux de la personne concernée. Cette référence sert plutôt à insister sur l'objectif général de la législation en matière de protection des données et de la directive elle-même. En effet, l'article 1er, paragraphe 1, mentionne non seulement la protection de la vie privée, mais aussi la protection des autres «libertés et droits fondamentaux des personnes physiques» dans leur ensemble, dont la vie privée n'est qu'une composante.

[6] Le 25 janvier 2012, la Commission européenne a adopté un paquet de mesures visant à réformer le cadre européen de la protection des données. Ce paquet comprend: i) une communication [COM(2012)9 final], ii) une proposition de règlement général en matière de protection des données (ci-après «le règlement proposé») [COM(2012)11 final], et iii) une proposition de directive sur la protection des données dans le secteur répressif [COM(2012)10 final]. L'analyse d'impact qui l'accompagne, comportant 10 annexes, est présentée dans un document de travail des services de la Commission [SEC(2012)72 final]. Voir, en particulier, l'étude intitulée «Evaluation of the implementation of the Data Protection Directive» (évaluation de la mise en œuvre de la directive sur la protection des données), qui constitue l'annexe 2 de l'analyse d'impact accompagnant le paquet de mesures de la Commission européenne visant à réformer le cadre européen de la protection des données.

[7] Voir page 8, dans la section II.1 «Bref historique», *«Mise en œuvre de la directive: l'arrêt ASNEF et FECEMD»*.

[8] Voir le programme de travail 2012-2013 du groupe de travail «Article 29», adopté le 1er février 2012 (WP 190).

Mettre en œuvre le cadre juridique actuel et préparer l'avenir

Le programme de travail a lui-même clairement défini deux objectifs: «assurer la mise en œuvre correcte du cadre juridique actuel» et aussi «préparer l'avenir».

En conséquence, le premier objectif du présent avis est d'assurer une compréhension commune du cadre juridique existant. Cet objectif s'inscrit dans le prolongement d'avis antérieurs portant sur d'autres dispositions-clés de la directive[9]. Dans un deuxième temps, en s'appuyant sur l'analyse proposée, l'avis formulera aussi des recommandations à prendre en considération lors du réexamen du cadre juridique sur la protection des données.

Structure de l'avis

Après un bref survol, au chapitre II, de l'histoire et du rôle de l'intérêt légitime et d'autres motifs légitimant le traitement, le chapitre III examinera et interprétera les dispositions concernées de la directive, en tenant compte de ce qui est constant dans leur application nationale. Cette analyse sera illustrée d'exemples pratiques tirés des expériences nationales. Elle étayera les recommandations formulées au chapitre IV tant en ce qui concerne l'application du cadre réglementaire actuel que dans le contexte de la révision de la directive.

II. Observations générales et considérations politiques

II.1. Bref historique

Cet aperçu examine plus particulièrement le développement des notions de licéité et de fondements juridiques justifiant le traitement, dont l'intérêt légitime. Il explique notamment comment la nécessité d'une base juridique a d'abord constitué une condition dans le contexte des dérogations au droit à la vie privée, avant de devenir une exigence distincte dans le contexte de la protection des données.

La Convention européenne des droits de l'homme («CEDH»)

L'article 8 de la Convention européenne des droits de l'homme, adoptée en 1950, consacre le droit au respect de la vie privée – à savoir le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il proscrit toute ingérence dans l'exercice de ce droit, sauf si elle est «prévue par la loi» et nécessaire «dans une société démocratique», afin de répondre à certains types d'intérêts publics impératifs, expressément énumérés.

L'article 8 de la CEDH traite en particulier de la protection de la vie privée et exige que toute ingérence soit justifiée. Cette approche repose sur une interdiction générale de l'ingérence dans l'exercice du droit à la vie privée et n'autorise des exceptions que dans des conditions strictement définies. En cas d'«ingérence dans la vie privée», une base juridique est requise, de même que la spécification d'une finalité légitime comme condition préalable permettant

[9] Comme l'avis 3/2013 sur la limitation de la finalité, adopté le 3.4.2013 (WP 203), l'avis 15/2011 sur la définition du consentement (cité en note de bas de page 2), l'avis 8/2010 sur le droit applicable, adopté le 16.12.2010 (WP 179) et l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16.2.2010 (WP 169).

d'apprécier la nécessité de l'ingérence. Cette approche explique que la CEDH ne dresse pas la liste des fondements juridiques possibles, mais se concentre sur la nécessité d'une base juridique et sur les conditions que cette base juridique doit remplir.

La Convention 108

La Convention 108[10] du Conseil de l'Europe, ouverte à la signature en 1981, introduit la notion distincte de protection des données à caractère personnel. L'idée sous-jacente, à l'époque, n'était pas que le traitement des données à caractère personnel devrait toujours être perçu comme une «*ingérence* dans la vie privée», mais plutôt que, pour *protéger* les droits et libertés fondamentaux de toute personne, et notamment son droit au respect de sa vie privée, le traitement des données à caractère personnel devrait toujours remplir certaines conditions. L'article 5 établit donc les principes fondamentaux du droit en matière de protection des données, notamment l'exigence selon laquelle les «données à caractère personnel faisant l'objet d'un traitement automatisé sont: a) obtenues et traitées loyalement et licitement». La Convention ne mentionnait toutefois pas de motifs détaillés justifiant le traitement[11].

Les lignes directrices de l'OCDE[12]

Élaborées parallèlement à la Convention 108 et adoptées en 1980, les lignes directrices de l'OCDE s'inscrivent dans des idées similaires de «licéité», bien que la notion soit exprimée de manière différente. Les lignes directrices ont été mises à jour en 2013, sans modification sensible du principe de licéité. Leur article 7 prévoit en particulier qu'«[i]l conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement». Le fondement juridique constitué par le consentement est ici expressément mentionné comme une possibilité, à laquelle il convient de recourir «le cas échéant». Cela suppose une appréciation des intérêts et des droits en jeu, ainsi qu'une évaluation de la mesure dans laquelle le traitement est intrusif. En ce sens, l'approche de l'OCDE présente certaines similitudes avec les critères – nettement plus élaborés – prévus par la directive 95/46/CE.

La directive 95/46/CE

Lors de son adoption, en 1995, la directive était inspirée des premiers instruments adoptés en matière de protection des données, notamment la Convention 108 et les lignes directrices de l'OCDE. L'expérience encore balbutiante acquise par certains États membres dans le domaine de la protection des données avait elle aussi été prise en considération.

Outre une exigence plus générale énoncée à son article 6, paragraphe 1, point a), selon laquelle les données à caractère personnel doivent être traitées «loyalement et licitement», la

[10] Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

[11] Le projet de texte de la Convention modernisée adopté en assemblée plénière par le T-PD en novembre 2012 prévoit que le traitement des données peut être effectué sur la base du consentement de la personne concernée ou en vertu «d'un autre fondement légitime prévu par la loi», à l'instar de la Charte des droits fondamentaux de l'Union européenne mentionnée ci-après en page 9.

[12] Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 11 juillet 2013.

directive ajoutait un ensemble spécifique de conditions supplémentaires, qui ne figuraient pas en tant que telles dans la Convention 108 ni dans les lignes directrices de l'OCDE: le traitement des données à caractère personnel doit être basé sur l'un des six fondements juridiques mentionnés à l'article 7.

Mise en œuvre de la directive: l'arrêt ASNEF et FECEMD[13]

Le rapport de la Commission intitulé «Evaluation of the implementation of the Data Protection Directive» (évaluation de la mise en œuvre de la directive sur la protection des données)[14] souligne que la mise en œuvre des dispositions de la directive dans le droit national s'est parfois révélée peu satisfaisante. Dans l'analyse technique de la transposition de la directive par les États membres[15], la Commission donne des précisions sur l'application de l'article 7. L'analyse explique que, si la législation de la plupart des États membres énonce les six fondements juridiques en termes relativement semblables à ceux utilisés dans la directive, la souplesse de ces principes a, dans les faits, conduit à des applications divergentes.

Dans ce contexte, il est particulièrement intéressant de relever que la Cour de justice a considéré, dans son arrêt ASNEF et FECEMD du 24 novembre 2011, que l'Espagne n'avait pas transposé correctement l'article 7, point f), de la directive en imposant – en l'absence du consentement de la personne concernée – que les données traitées figurent dans des sources accessibles au public. L'arrêt déclarait en outre que l'article 7, point f), a un effet direct. L'arrêt limite la marge d'appréciation dont disposent les États membres pour appliquer l'article 7, point f). En particulier, ils ne doivent pas franchir la ligne ténue qui sépare, d'un côté, la clarification et, de l'autre, la formulation d'exigences supplémentaires, qui reviendrait à modifier le champ d'application de l'article 7, point f).

L'arrêt, en ce qu'il précise que les États membres ne sont pas autorisés à imposer des restrictions et exigences unilatérales supplémentaires quant aux fondements juridiques du traitement licite des données dans leur droit national, a des conséquences non négligeables. Les juridictions nationales et autres organes concernés doivent interpréter les dispositions nationales à la lumière de cet arrêt et, si nécessaire, écarter les règles et les pratiques non conformes.

Cet arrêt montre combien il importe que les autorités nationales chargées de la protection des données et/ou les législateurs européens parviennent à une compréhension claire et commune de l'applicabilité de l'article 7, point f). Il convient pour ce faire d'adopter une approche équilibrée, qui ne restreint ni n'élargit indument le champ d'application de cette disposition.

La Charte des droits fondamentaux

Depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») a «la même valeur juridique que les traités»[16]. Son article 8 consacre la protection des données à caractère personnel comme un droit fondamental, distinct du droit au respect de sa vie privée et familiale, qui fait l'objet de

[13] Arrêt de la Cour de justice du 24.11.2011 dans les affaires C-468/10 et C-469/10 (ASNEF et FECEMD).
[14] Voir l'annexe 2 de l'analyse d'impact accompagnant le paquet de mesures de la Commission européenne visant à réformer le cadre européen de protection des données, cité précédemment, en note de bas de page 6.
[15] Analyse et étude d'impact sur la mise en œuvre de la directive 95/46/CE dans les États membres. Voir http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

l'article 7. Il énonce l'exigence d'un fondement légitime pour le traitement. Concrètement, il prévoit que les données à caractère personnel doivent être traitées «sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi»[17]. Ces dispositions renforcent aussi bien l'importance du principe de licéité que la nécessité de justifier le traitement des données à caractère personnel par une base juridique adéquate.

La proposition de règlement sur la protection des données

Dans le contexte du processus de révision du cadre de la protection des données, la portée des motifs fondant la licéité du traitement prévus à l'article 7, et en particulier le champ d'application de l'article 7, point f), font actuellement l'objet de discussions.

L'article 6 du règlement proposé énumère les motifs justifiant un traitement licite des données à caractère personnel. À quelques exceptions près (qui seront décrites plus loin), les six motifs susceptibles d'être invoqués demeurent largement inchangés par rapport à ceux actuellement prévus par l'article 7 de la directive. La Commission a cependant proposé de fournir des orientations supplémentaires sous la forme d'actes délégués.

Il est intéressant de noter que, dans le cadre des travaux de la commission du Parlement européen concernée[18], les députés se sont efforcés de clarifier la notion d'intérêt légitime dans la proposition de règlement elle-même. Une liste de cas dans lesquels l'intérêt légitime poursuivi par le responsable du traitement des données prévaudrait en principe sur l'intérêt légitime et les droits et libertés fondamentaux de la personne concernée a été dressée, ainsi qu'une deuxième liste de cas où ce serait l'inverse. Ces listes – mentionnées dans les dispositions ou dans les considérants – apportent une contribution utile pour apprécier l'équilibre entre les droits et intérêts du responsable du traitement et ceux de la personne concernée. Elles sont prises en compte dans le présent avis[19].

[16] Voir l'article 6, paragraphe 1, du TUE.
[17] Voir l'article 8, paragraphe 2, de la Charte.
[18] Projet de rapport de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)], daté du 16.1.2013 (ci-après le «projet de rapport de la commission LIBE»). Voir, en particulier, les amendements 101 et 102. Voir aussi les amendements adoptés par la commission le 21.10.2013 dans son rapport final (ci-après le «rapport final de la commission LIBE»).
[19] Voir la section III.3.1 et, en particulier, la liste à puces en pages 27 et 28 énumérant de façon non exhaustive certains des contextes où la question de l'intérêt légitime au sens de l'article 7, point f), est le plus communément susceptible de se poser.

II.2. Le rôle de la notion

L'intérêt légitime poursuivi par le responsable du traitement: le critère de la mise en balance en dernier recours?

L'article 7, point f), constitue la dernière option parmi les six motifs qui rendent licite le traitement des données à caractère personnel. Il impose un critère reposant sur une mise en balance: ce qui est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (ou par les tiers) doit être mis en balance avec l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le résultat de cette mise en balance détermine si l'article 7, point f), peut servir de fondement juridique au traitement.

Le caractère ouvert de cette disposition suscite maintes questions importantes concernant sa portée exacte et son application, qui seront analysées successivement dans le présent avis. Toutefois, ainsi qu'il est expliqué ci-après, cette option ne doit pas pour autant être perçue comme pouvant uniquement être utilisée avec parcimonie pour combler les lacunes «en dernier ressort» dans des situations rares et imprévues, ou comme une dernière chance si aucun autre motif ne s'applique. Elle ne doit pas non plus apparaître comme une option privilégiée, ni son utilisation être indument encouragée pour la simple raison qu'elle est considérée comme moins contraignante que les autres motifs.

Il se pourrait bien, au contraire, que l'article 7, point f), ait, de par sa nature même, un intérêt propre et qu'il ait un rôle très utile à jouer comme motif fondant la licéité du traitement, si plusieurs conditions déterminantes sont remplies.

Un recours approprié à l'article 7, point f), dans les circonstances appropriées et moyennant des garanties adéquates, permet aussi d'éviter un mauvais usage et une invocation excessive d'autres fondements juridiques.

Les cinq premiers motifs de l'article 7 reposent sur le consentement de la personne concernée, sur une disposition contractuelle, sur une obligation légale ou sur d'autres justifications expressément identifiées comme conférant au traitement sa légitimité. Quand le traitement est fondé sur l'un de ces cinq motifs, il est considéré a priori comme légitime et donc uniquement subordonné au respect d'autres dispositions du droit applicables. Autrement dit, l'équilibre entre les différents droits et intérêts en jeu – y compris ceux du responsable du traitement et de la personne concernée – est présumé atteint, à condition, bien sûr, que toutes les autres dispositions du droit en matière de protection des données soient respectées. L'article 7, point f), quant à lui, impose un critère *spécifique*, dans les cas qui ne cadrent pas avec les scénarios prédéfinis des motifs a) à e). Il assure que tout traitement, en dehors de ces scénarios, doive répondre aux exigences d'un critère de mise en balance, en tenant dûment compte des intérêts et droits fondamentaux de la personne concernée.

Ce critère peut, dans certains cas, mener à la conclusion que la balance penche en faveur des intérêts et droits fondamentaux des personnes concernées et que, par conséquent, le traitement ne peut être effectué. D'un autre côté, une évaluation appropriée de l'équilibre requis par l'article 7, point f), souvent assortie d'une possibilité de s'opposer au traitement, peut, dans d'autres cas, être préférable à l'invocation inappropriée, par exemple, du motif du «consentement» ou du caractère «nécessaire à l'exécution d'un contrat». Vu sous cet angle, l'article 7, point f), présente des garanties complémentaires – qui imposent des mesures appropriées – par rapport aux autres motifs prédéfinis. Il ne doit donc pas être considéré

comme «le maillon faible» ni comme une porte ouverte à la légitimation de tous les traitements de données qui ne relèvent d'aucun des autres fondements juridiques.

Le groupe de travail insiste sur le fait que son interprétation du champ d'application de l'article 7, point f), vise à proposer une approche équilibrée, qui garantisse aux responsables du traitement des données la flexibilité nécessaire dans les situations où les personnes concernées ne subissent pas une incidence injustifiée, tout en offrant à ces personnes une sécurité juridique et des garanties suffisantes pour empêcher tout abus de cette disposition ouverte.

II.3. Les notions liées

La relation de l'article 7, point f), avec d'autres motifs fondant la licéité du traitement

L'article 7 commence par le consentement, et continue en énumérant les autres motifs fondant la licéité du traitement, dont les contrats et obligations légales, pour en arriver progressivement au critère de l'intérêt légitime, qui figure en dernière position parmi les six motifs susceptibles d'être invoqués. L'ordre dans lequel les fondements juridiques sont présentés à l'article 7 a parfois été interprété comme une indication de l'importance respective des différents motifs. Cependant, comme le groupe de travail l'a déjà souligné dans son avis sur la notion de consentement[20], le libellé de la directive n'établit pas de distinction juridique entre les six motifs et n'indique aucunement qu'il existe entre eux une hiérarchie. Rien n'indique que l'article 7, point f), ne doive être appliqué que dans des cas exceptionnels, et aucun autre élément dans le libellé ne suggère que l'ordre spécifique des six fondements juridiques ait un quelconque effet juridiquement pertinent. Néanmoins, la signification précise de l'article 7, point f), et sa relation avec d'autres motifs fondant la licéité du traitement sont longtemps demeurées assez obscures.

Dans ce contexte, diverses approches, favorisées par la formulation ouverte de la directive, sont apparues au gré des diversités historiques et culturelles: certains États membres ont eu tendance à envisager l'article 7, point f), comme un motif d'ordre inférieur, destiné à combler les lacunes uniquement dans des cas exceptionnels où aucun des cinq autres motifs ne s'appliquerait[21]. D'autres États membres, à l'inverse, n'y voient qu'une possibilité parmi six autres, qui n'est ni plus ni moins importante que les autres options et qui peut s'appliquer à des situations très nombreuses et variées, pour autant que les conditions nécessaires soient remplies.

Compte tenu de ces divergences, et également de l'arrêt ASNEF et FECEMD, il importe de clarifier la relation de «l'intérêt légitime» avec les autres motifs fondant la licéité du traitement – c'est-à-dire, par exemple, avec le consentement, les clauses contractuelles, les missions d'intérêt public – ainsi qu'avec le droit d'opposition de la personne concernée. On pourrait ainsi mieux définir le rôle et la fonction du motif de l'intérêt légitime et donc apporter plus de sécurité juridique.

[20] Voir la note de bas de page 2 ci-dessus.

[21] Il est aussi à noter que le projet de rapport de la commission LIBE proposait, par son amendement 100, de séparer l'article 7, point f), des autres fondements juridiques et aussi d'ajouter des exigences supplémentaires au cas où ce fondement juridique est invoqué, notamment un renforcement de la transparence et de la responsabilité, comme on le verra plus tard.

Il faut aussi relever que le motif de l'intérêt légitime, à l'instar des autres motifs hormis celui du consentement, comporte un critère de «nécessité» qui doit être rempli. Cela limite strictement le contexte dans lequel chacun de ces motifs peut s'appliquer. La Cour de justice de l'Union européenne a considéré que la «nécessité» constitue une notion autonome du droit communautaire[22]. La Cour européenne des droits de l'homme a, elle aussi, donné des orientations utiles[23].

De surcroît, le fait d'avoir un fondement juridique approprié ne dispense pas le responsable du traitement des données de respecter les obligations de loyauté, de licéité, de nécessité et de proportionnalité, mais aussi de qualité des données, qui lui incombent en vertu de l'article 6. Par exemple, même si le traitement des données à caractère personnel est justifié par l'intérêt légitime ou par l'exécution d'un contrat, cela n'autorise pas une collecte de données excessive au regard de la finalité spécifiée.

L'intérêt légitime et les autres motifs visés à l'article 7 sont des motifs alternatifs et il suffit donc qu'un seul d'entre eux s'applique. Cependant, ils viennent s'ajouter non seulement aux exigences de l'article 6, mais aussi à tous les autres principes et obligations de protection des données qui peuvent être applicables.

Autres critères de mise en balance

L'article 7, point f), n'est pas le seul critère de mise en balance prévu dans la directive. Par exemple, l'article 9 suppose un équilibre entre le droit à la protection des données à caractère personnel et la liberté d'expression. Cet article permet aux États membres d'accorder des exemptions et dérogations pour les traitements des données à caractère personnel «effectués aux seules fins de journalisme ou d'expression artistique ou littéraire» si elles sont «nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression».

De plus, de nombreuses autres dispositions de la directive requièrent aussi une analyse au cas par cas, une mise en balance des intérêts et des droits en jeu et une certaine souplesse dans l'appréciation de multiples facteurs. Il s'agit notamment des dispositions relatives à la nécessité, à la proportionnalité et à la limitation de la finalité, aux exceptions visées à l'article 13, et à la recherche scientifique, pour n'en citer que quelques-unes.

Il semble effectivement que la directive ait été conçue pour laisser place à l'interprétation et à la mise en balance des intérêts. L'intention était bien sûr, au moins en partie, de donner aux États membres une marge de manœuvre plus grande pour la transposition dans le droit national. Cependant, la nécessité d'une certaine flexibilité découle, en outre, de la nature

[22] Arrêt de la Cour de justice du 16 décembre 2008, dans l'affaire C-524/06 (Heinz Huber/Bundesrepublik Deutschland), point 52: «Dès lors, eu égard à l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres, la notion de nécessité telle qu'elle résulte de l'article 7, sous e), de la directive 95/46, qui vise à délimiter précisément une des hypothèses dans lesquelles le traitement de données à caractère personnel est licite, ne saurait avoir un contenu variable en fonction des États membres. Partant, il s'agit d'une notion autonome du droit communautaire qui doit recevoir une interprétation de nature à répondre pleinement à l'objet de cette directive tel que défini à l'article 1er, paragraphe 1, de celle-ci.»

[23] Arrêt de la Cour européenne des droits de l'homme du 25 mars 1983, dans l'affaire Silver et autres/Royaume-Uni, au point 97 à propos de l'expression «nécessaire dans une société démocratique»: «l'adjectif "nécessaire" n'est pas synonyme d'"indispensable", mais n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" […].»

même du droit à la protection des données à caractère personnel et du droit au respect de la vie privée. En effet, ces deux droits, de même que la plupart (mais non la totalité) des autres droits fondamentaux, sont considérés comme des droits humains relatifs, ou qualifiés[24]. Les droits de ce type doivent toujours être interprétés dans leur contexte. Pour autant que des garanties appropriées soient prévues, ils peuvent être mis en balance avec les droits d'autrui. Dans certaines situations – toujours sous réserve de garanties appropriées – ils peuvent aussi être soumis à des restrictions pour des raisons d'intérêt public.

II.4. Contexte et conséquences stratégiques

Garantir la légitimité mais aussi la flexibilité: les moyens de préciser l'article 7, point f)

Le libellé actuel de l'article 7, point f), de la directive est ouvert. Il s'ensuit qu'il peut servir de fondement dans un large éventail de situations, du moment que ses exigences sont satisfaites, et notamment le critère de mise en balance. Cependant, une telle flexibilité peut aussi avoir des conséquences négatives. Des orientations complémentaires seraient donc utiles pour éviter une application incohérente de la directive dans les États membres ou un manque de sécurité juridique.

La Commission prévoit de telles orientations dans la proposition de règlement, sous la forme d'actes délégués. D'autres options consistent notamment à apporter des éclaircissements et introduire des dispositions détaillées dans le texte du règlement proposé lui-même[25] et/ou à confier au comité européen de la protection des données le soin de formuler des orientations complémentaires dans ce domaine.

Chacune de ces options a des avantages et des inconvénients. Si l'appréciation devait avoir lieu au cas par cas, sans autres orientations, cela risquerait d'entraîner une application incohérente et un manque de prévisibilité, comme c'était le cas précédemment.

D'un autre côté, le fait de prévoir, dans le texte même du règlement proposé, des listes détaillées et exhaustives de situations dans lesquelles l'intérêt légitime poursuivi par le responsable du traitement prévaut en règle générale sur les droits fondamentaux de la personne concernée, ou inversement, pourrait induire en erreur ou être inutilement coercitif, ou les deux à la fois.

Ces approches pourraient néanmoins inspirer une solution équilibrée, apportant certaines précisions complémentaires dans le règlement proposé lui-même et d'autres orientations dans des actes délégués ou dans les lignes directrices du comité européen de la protection des données[26].

---

[24] Il n'existe que peu de droits humains qui ne puissent être mis en balance avec les droits d'autrui ou avec l'intérêt collectif. On les appelle les droits absolus. Ces droits ne peuvent jamais être limités ni restreints, quelles que soient les circonstances – même en cas de guerre ou d'état d'urgence. Le droit de n'être pas soumis à la torture ni à un traitement inhumain ou dégradant en est un exemple. Il n'est jamais admissible de torturer quelqu'un ou de le traiter d'une manière inhumaine ou dégradante, quelles que soient les circonstances. Les exemples de droits humains non absolus comprennent notamment le droit au respect de la vie privée et familiale, le droit à la liberté d'expression et le droit à la liberté de pensée, de conscience et de religion.

[25] Voir la section II.1 «Bref historique», *«La proposition de règlement sur la protection des données»*, en page 9.

[26] En ce qui concerne les actes délégués et les orientations du comité européen de la protection des données, le groupe de travail «Article 29» a fait part, dans son avis 08/2012 apportant des contributions supplémentaires au

L'analyse présentée au chapitre III vise à jeter les bases d'une telle approche, ni trop générale au point d'en perdre toute signification, ni trop précise au point d'en devenir exagérément rigide.

III. Analyse des dispositions

III.1. Aperçu général de l'article 7

L'article 7 dispose que le traitement de données à caractère personnel ne peut être effectué que si au moins un des six motifs juridiques énumérés à cet article s'applique. Avant d'analyser chacun de ces motifs, la section III.1 donne un aperçu général de l'article 7 et de sa relation avec l'article 8, qui porte sur les catégories particulières de données.

III.1.1. Consentement ou «nécessaire à...»

Une distinction peut être établie entre le cas où le traitement des données à caractère personnel se fonde sur le consentement indubitable de la personne concernée [article 7, point a)] et les cinq autres cas [article 7, points b) à f)]. En résumé, ces derniers décrivent des scénarios où le traitement peut se révéler nécessaire dans un contexte spécifique, comme l'exécution d'un contrat conclu avec la personne concernée, le respect d'une obligation légale imposée au responsable du traitement, etc.

Dans le premier cas, visé à l'article 7, point a), ce sont les personnes concernées elles-mêmes qui autorisent le traitement de leurs données à caractère personnel. Il leur appartient de décider si elles permettent que leurs données soient traitées. Le consentement n'élimine pas pour autant la nécessité de respecter les principes énoncés à l'article 6[27]. De plus, le consentement doit encore remplir certaines conditions essentielles pour être légitime, comme l'explique l'avis 15/2011 du groupe de travail[28]. Dès lors que le traitement des données de l'utilisateur est, en définitive, laissé à sa discrétion, tout dépend de la validité et de la portée du consentement de la personne concernée.

Autrement dit, le premier motif, mentionné à l'article 7, point a), a trait à l'autodétermination de la personne concernée comme fondement de la légitimité. Tous les autres motifs, en revanche, autorisent le traitement – moyennant des garanties et des mesures définies – dans des situations où, indépendamment du consentement, il est approprié et nécessaire de traiter les données dans un certain contexte pour servir un intérêt légitime spécifique.

---

débat sur la réforme de la protection des données, adopté le 5.10.2012 (WP 199), de sa nette préférence pour les orientations (voir p. 14 et 15).

[27] Arrêt de la Cour suprême des Pays-Bas du 9 septembre 2011 dans l'affaire ECLI:NL:HR:2011:BQ8097, point 3.3, e), à propos du principe de proportionnalité. Voir aussi la page 8 de l'avis 15/2011 du groupe de travail «Article 29», cité en note de bas de page 2, ci-dessus: «[...] l'obtention d'un consentement n'annule pas les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière.»

[28] Voir les pages 12 à 28 de l'avis 15/2011, cité en note 2 ci-dessus.

Les points b), c), d) et e) spécifient chacun un critère légitimant le traitement:

b) l'exécution d'un contrat conclu avec la personne concernée;
c) le respect d'une obligation légale imposée au responsable du traitement;
d) la sauvegarde de l'intérêt vital de la personne concernée;
e) l'exécution d'une mission d'intérêt public.

Le point f) est moins précis et renvoie, plus généralement, à un (quelconque) intérêt légitime poursuivi par le responsable du traitement (dans n'importe quel contexte). Cette disposition générale est cependant expressément subordonnée à un critère supplémentaire de mise en balance, qui vise à protéger l'intérêt et les droits des personnes concernées, comme on le verra à la section III.2.

Dans tous les cas, c'est au responsable du traitement des données qu'il revient initialement d'apprécier si les critères énoncés à l'article 7, points a) à f), sont remplis, sous réserve du respect du droit applicable et des orientations relatives à la façon dont ce droit doit être appliqué. Ensuite, la légitimité du traitement peut faire l'objet d'une autre évaluation, et éventuellement être contestée, par les personnes concernées, par d'autres parties prenantes, par les autorités chargées de la protection des données, et en définitive la question peut être tranchée par les tribunaux.

Pour compléter ce bref aperçu, il convient d'indiquer que, comme on le verra à la section III.3.6, au moins dans les cas visés aux points e) et f), la personne concernée peut exercer son droit d'opposition, ainsi que le prévoit l'article 14[29]. Cela donnera lieu à une nouvelle évaluation des intérêts en jeu ou, si le traitement des données à caractère personnel est envisagé à des fins de prospection [article 14, point b)], cela contraindra le responsable du traitement à y mettre un terme, sans évaluation complémentaire.

III.1.2. Relation avec l'article 8

L'article 8 de la directive régit de façon plus détaillée le traitement de certaines catégories particulières de données à caractère personnel. Il concerne plus spécialement le traitement des données «qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle» (article 8, paragraphe 1), et les données «relatives aux infractions [ou] aux condamnations pénales» (article 8, paragraphe 5).

Le traitement de ces données est en principe interdit, sous réserve de certaines exceptions. L'article 8, paragraphe 2, prévoit plusieurs exceptions à cette interdiction, aux points a) à e). L'article 8, paragraphes 3 et 4, prévoit d'autres exceptions. Certaines de ces dispositions sont analogues – mais non identiques – à celles énoncées à l'article 7, points a) à f).

[29] Selon l'article 14, point a), ce droit s'applique «sauf en cas de disposition contraire du droit national». En Suède, par exemple, le droit national ne reconnaît pas la possibilité de s'opposer à un traitement fondé sur l'article 7, point e).

Les conditions spécifiques de l'article 8, ainsi que le fait que certains des motifs énumérés à l'article 7 ressemblent aux conditions énoncées à l'article 8, conduisent à s'interroger sur la relation entre les deux dispositions.

Si l'article 8 est conçu comme une *lex specialis*, il convient d'examiner s'il exclut complètement l'applicabilité de l'article 7. Dans l'affirmative, cela signifierait que des catégories particulières de données à caractère personnel peuvent être traitées sans que les critères de l'article 7 doivent être satisfaits, pour autant qu'une des exceptions de l'article 8 s'applique. Il est cependant également possible que la relation soit plus complexe et que les articles 7 et 8 doivent être appliqués cumulativement[30].

Quoi qu'il en soit, il est clair que l'objectif de la mesure est d'assurer une protection supplémentaire pour des catégories particulières de données. Par conséquent, le résultat final de l'analyse devrait être tout aussi clair: l'application de l'article 8, en soi ou cumulé avec l'article 7, vise à garantir un niveau de protection plus élevé de certaines catégories particulières de données.

Dans la pratique, bien que, dans certains cas, l'article 8 énonce des exigences plus strictes – comme le consentement «explicite» requis à l'article 8, paragraphe 2, point a), par rapport au consentement «indubitablement donné» prévu à l'article 7 – il n'en va pas ainsi de toutes les dispositions. Certaines exceptions prévues par l'article 8 ne semblent pas équivalentes ou plus strictes que les motifs visés à l'article 7. Il serait inapproprié de conclure, par exemple, que le fait que des catégories particulières de données ont été manifestement rendues publiques par quelqu'un, comme l'envisage l'article 8, paragraphe 2, point e), serait – toujours et en soi – une condition suffisante pour autoriser tout type de traitement des données, sans mettre en balance les intérêts et les droits en jeu, comme l'exige l'article 7, point f)[31].

Dans certaines situations, le fait que le responsable du traitement des données soit un parti politique lèverait aussi l'interdiction du traitement de catégories particulières de données selon l'article 8, paragraphe 2, point d). Cela ne veut pas dire pour autant que tout traitement entrant dans le champ d'application de cette disposition soit nécessairement licite. Cette question doit être appréciée séparément et le responsable du traitement devra éventuellement démontrer, par exemple, que le traitement des données est nécessaire à l'exécution d'un contrat [article 7, point b)], ou que son intérêt légitime prévaut, conformément à l'article 7, point f). Dans ce dernier cas, le critère de mise en balance prévu par l'article 7, point f), doit être appliqué après l'appréciation du respect des exigences de l'article 8 par le responsable du traitement des données.

De même, le simple fait que «le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la

[30] Puisque l'article 8 se présente comme *une interdiction avec des exceptions*, celles-ci peuvent être perçues comme des exigences, qui limitent seulement la portée de l'interdiction mais ne constituent pas, en tant que telles, un fondement juridique suffisant pour justifier le traitement. Selon cette lecture, l'applicabilité des exceptions de l'article 8 n'exclut pas l'applicabilité des exigences de l'article 7, et les unes comme les autres doivent, le cas échéant, s'appliquer cumulativement.

[31] De plus, l'article 8, paragraphe 2, point e), ne saurait être interprété a contrario comme signifiant que, si les données rendues publiques par la personne concernée ne sont pas des données sensibles, elles peuvent être traitées sans satisfaire à d'autres conditions. Les données accessibles au public restent des données à caractère personnel soumises aux exigences de la protection des données, notamment au respect de l'article 7, qu'il s'agisse ou non de données sensibles.

gestion de services de santé» et l'obligation de secret qui s'applique au traitement de ces données – comme indiqué à l'article 8, paragraphe 3 – impliquent qu'un tel traitement de données sensibles est *exempté de l'interdiction* visée à l'article 8, paragraphe 1. Ce n'est pourtant pas nécessairement suffisant pour garantir aussi la licéité au titre de l'article 7, et un fondement juridique comme l'exécution d'un contrat conclu avec le patient conformément à l'article 7, point b), une obligation légale conformément à l'article 7, point c), l'exécution d'une mission d'intérêt public conformément à l'article 7, point e), ou l'appréciation du critère énoncé à l'article 7, point f), sera requis.

En conclusion, le groupe de travail considère qu'il faut analyser au cas par cas si l'article 8 prévoit, en soi, des conditions plus strictes et suffisantes[32], ou s'il convient d'appliquer cumulativement les articles 8 et 7 pour garantir une protection complète des personnes concernées. Le résultat de l'examen ne peut en aucun cas aboutir à une moindre protection des catégories particulières de données[33].

Il s'ensuit aussi que le responsable du traitement qui s'occupe de catégories particulières de données ne peut jamais invoquer *uniquement* un fondement juridique relevant de l'article 7 pour légitimer une activité de traitement des données. Le cas échéant, l'article 7 ne *prévaudra* pas, mais s'appliquera toujours de manière *cumulative* avec l'article 8, afin que toutes les garanties et les mesures pertinentes soient respectées. Cela vaudra d'autant plus dans les cas où les États membres décident d'ajouter des exemptions à celles énoncées à l'article 8, ainsi que le prévoit l'article 8, paragraphe 4.

III.2. Article 7, points a) à e)

La présente section III.2 donne un bref aperçu de chacun des fondements juridiques mentionnés à l'article 7, points a) à e), de la directive, avant d'examiner plus particulièrement, à la section III.3, l'article 7, point f). Cette analyse mettra aussi en lumière certaines des corrélations les plus courantes entre ces fondements juridiques, faisant intervenir par exemple un «contrat», une «obligation légale» et un «intérêt légitime», selon le contexte particulier et les circonstances.

III.2.1. Consentement

Le consentement, en tant que fondement juridique, a été analysé dans l'avis 15/2011 du groupe de travail sur la définition du consentement. L'avis concluait essentiellement que le consentement n'est qu'un fondement juridique parmi d'autres, plutôt que le fondement principal légitimant le traitement de données à caractère personnel. Il joue un rôle important mais n'exclut pas la possibilité que, compte tenu du contexte, d'autres fondements juridiques puissent être jugés plus appropriés par le responsable du traitement ou par la personne concernée. S'il est utilisé à bon escient, le consentement est un instrument qui permet à la

[32] Voir l'analyse présentée dans l'avis «AMA» du groupe de travail «Article 29», point 3.3, qui prend en considération aussi bien l'article 7 que l'article 8 de la directive: Deuxième avis 4/2009 sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage, adopté le 6.4.2009 (WP 162).

[33] Il va sans dire que, dans le cas de l'application de l'article 8 également, le respect des autres dispositions de la directive, y compris son article 6, doit être assuré.

personne concernée de contrôler le traitement de ses données. Au contraire, s'il est mal utilisé, le contrôle de la personne concernée devient illusoire et le consentement constitue alors une base inappropriée pour le traitement de données.

Parmi ses recommandations, le groupe de travail soulignait la nécessité de clarifier le sens de la notion de «consentement indubitable»: «[c]ette clarification devrait insister sur le fait qu'un consentement indubitable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement. Dans le même temps, il conviendrait d'expliquer que l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement (consentement fondé sur le silence), ne constitue pas, en soi, un consentement indubitable. Cette observation vaut tout particulièrement dans l'environnement en ligne[34].» Il proposait aussi d'exiger des responsables du traitement qu'ils mettent en place des mécanismes pour démontrer le consentement (dans le cadre de l'obligation générale de rendre compte) et invitait le législateur à ajouter une exigence explicite concernant la qualité et l'accessibilité des informations servant de base au consentement.

III.2.2. Contrat

L'article 7, point b), constitue un fondement juridique dans les situations où le traitement «est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci». Cela recouvre deux scénarios différents.

i) Dans le premier cas de figure, la disposition s'applique aux situations dans lesquelles le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. Il peut s'agir, par exemple, du traitement de son adresse pour que des produits achetés en ligne puissent être livrés, ou du traitement des informations figurant sur une carte de crédit afin d'effectuer une transaction. Dans le contexte des relations de travail, ce motif peut autoriser, par exemple, le traitement des informations relatives aux salaires et des coordonnées de comptes bancaires pour que les salariés puissent être payés.

   La disposition doit être interprétée de façon restrictive et ne couvre pas les situations dans lesquelles le traitement n'est pas véritablement *nécessaire* à l'exécution d'un contrat, mais plutôt imposé unilatéralement à la personne concernée par le responsable du traitement. Le fait qu'un certain traitement de données soit couvert par un contrat ne signifie pas non plus automatiquement que le traitement soit nécessaire à son exécution. Par exemple, l'article 7, point b), ne peut pas servir de fondement juridique pour établir un profil des goûts et du mode de vie de l'utilisateur à partir de son historique de navigation sur un site internet et des articles achetés. En effet, le responsable du traitement des données n'a pas été chargé, dans le contrat, d'établir un profil mais de fournir des produits et des services, par exemple. Même si ces activités de traitement sont expressément mentionnées en petits caractères dans le contrat, elles n'en deviennent pas pour autant «nécessaires» à l'exécution de ce dernier.

[34] Voir la page 41 de l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement.

Il existe ici un lien évident entre l'appréciation de la nécessité et le respect du principe de limitation de la finalité. Il importe de déterminer la raison d'être exacte du contrat, c'est-à-dire sa substance et son objectif fondamental, car c'est ce qui permettra de vérifier si le traitement des données est nécessaire à l'exécution du contrat.

Dans certaines situations limites, on peut être amené à s'interroger ou à recueillir des éléments complémentaires plus précis, afin de déterminer si le traitement est nécessaire à l'exécution du contrat. Ainsi, la constitution d'une base de données de contact à usage interne contenant les noms, les adresses professionnelles, les numéros de téléphone et les adresses de courrier électronique de tous les salariés d'une entreprise, destinée à faciliter les échanges d'informations entre collègues, peut dans certains cas être considérée comme nécessaire à l'exécution d'un contrat au titre de l'article 7, point b), mais elle peut aussi être licite en vertu de l'article 7, point f), s'il est démontré que l'intérêt du responsable du traitement prévaut et si toutes les mesures appropriées ont été prises, par exemple, en consultant dûment les représentants du personnel.

D'autres cas, comme la surveillance électronique de l'utilisation de l'internet, du courriel ou du téléphone par les salariés, ou la vidéosurveillance de ces derniers, constituent plus manifestement un traitement qui risque d'aller au-delà de ce qui est nécessaire à l'exécution d'un contrat de travail, bien que cela puisse, ici aussi, dépendre de la nature de l'emploi. La prévention de la fraude – qui peut inclure, entre autres, la surveillance et l'établissement de profils des clients – est un autre aspect généralement susceptible d'être considéré comme allant au-delà de ce qui est nécessaire à l'exécution d'un contrat. Un tel traitement pourrait tout de même être légitime en vertu d'un autre motif mentionné à l'article 7, par exemple, selon les circonstances, le consentement, une obligation légale ou l'intérêt légitime du responsable du traitement [article 7, point a, c) ou f)][35]. Dans ce dernier cas, le traitement devrait être subordonné à des garanties et mesures supplémentaires en vue de protéger l'intérêt ou les droits et libertés des personnes concernées.

L'article 7, point b), s'applique uniquement à ce qui est nécessaire à *l'exécution* d'un contrat. Il ne couvre pas les diverses actions déclenchées par le non-respect du contrat ni quelque autre incident dans son exécution. Tant que le traitement relève de l'exécution normale d'un contrat, il peut entrer dans le champ d'application de l'article 7, point b). S'il survient un incident qui donne lieu à un conflit, le traitement des données peut prendre un cours différent. Le traitement des informations de base relatives à la personne concernée, comme le nom, l'adresse et la référence à des obligations contractuelles en souffrance, pour l'envoi de rappels, devrait encore être considéré comme relevant du traitement de données nécessaire à l'exécution d'un

[35] Un autre exemple de fondements juridiques multiples est présenté dans l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement (cité en note de bas de page 2). Pour l'achat d'une voiture, le responsable du traitement peut être habilité à traiter des données à caractère personnel à différentes fins et sur la base de différents motifs:
- les données sont nécessaires à l'achat de la voiture: article 7, point b);
- pour traiter les documents du véhicule: article 7, point c);
- pour les services de gestion de la clientèle (par exemple, pour l'entretien du véhicule dans différentes entreprises du même groupe au sein de l'UE): article 7, point f);
- pour transférer les données à des tiers aux fins de leurs propres activités de commercialisation: article 7, point a).

contrat. Quant aux traitements plus élaborés de données, dans lesquels des tiers peuvent ou non intervenir, comme le recouvrement de créances, ou une action en justice à l'encontre d'un client en défaut de paiement, on pourrait faire valoir qu'un tel traitement ne relève plus de l'exécution «normale» du contrat et n'entre donc plus dans le champ d'application de l'article 7, point b). Cela ne rendrait cependant pas le traitement illégitime pour autant, car le responsable du traitement a un intérêt légitime à former un recours pour faire respecter ses droits contractuels. D'autres fondements juridiques, comme l'article 7, point f), pourraient être invoqués, sous réserve de garanties et de mesures appropriées, et du respect du critère de mise en balance[36].

ii) Dans le second cas de figure, l'article 7, point b), couvre aussi le traitement de données qui a lieu *avant* la conclusion d'un contrat. Il peut donc s'appliquer aux relations précontractuelles, pour autant que les démarches soient accomplies à la demande de la personne concernée, plutôt qu'à l'initiative du responsable du traitement ou d'un tiers. Par exemple, si une personne demande à un détaillant de lui faire une offre de prix pour un produit, le traitement de données effectué à cette fin, tel que la conservation, pour une durée limitée, de l'adresse et des informations à propos de ce qui est demandé, pourra s'appuyer sur ce fondement juridique. De même, si quelqu'un demande un devis à un assureur pour sa voiture, l'assureur est en droit de traiter les données nécessaires, par exemple, la marque et l'âge de la voiture, ainsi que d'autres données pertinentes et proportionnées, afin d'établir le devis.

En revanche, des vérifications détaillées comme, par exemple, le traitement de données d'examens médicaux par une compagnie d'assurances avant de proposer une assurance maladie ou une assurance vie ne seraient pas considérées comme une étape nécessaire accomplie à la demande de la personne concernée. Les vérifications de la cote de crédit avant d'accorder un prêt ne sont pas non plus effectuées *à la demande* de la personne concernée conformément à l'article 7, point b), mais plutôt au titre de l'article 7, point f), ou de l'article 7, point c), en vertu d'une obligation légale faite aux banques de consulter une liste officielle de débiteurs enregistrés.

Le traitement à des fins de prospection directe sur l'initiative du détaillant/responsable du traitement ne pourra pas non plus s'appuyer sur ce motif. Dans certains cas, l'article 7, point f), pourrait se substituer à l'article 7, point b), en tant que fondement juridique, sous réserve de garanties et de mesures appropriées, et du respect du critère de mise en balance. Dans d'autres circonstances, notamment en cas d'établissement de profils détaillés, de partage de données, de prospection directe en ligne ou de publicité comportementale, il convient d'examiner si la personne concernée a donné son consentement, conformément à l'article 7, point a), comme le montre l'analyse présentée plus bas[37].

III.2.3. Obligation légale

L'article 7, point c), constitue un fondement juridique dans les situations où le traitement «est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est

[36] Pour les catégories particulières de données, il convient peut-être aussi être de prendre en compte l'article 8, paragraphe 1, point e): «nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice».

[37] Voir la section III.3.6, point b), sous l'intitulé: «Illustration: l'évolution de l'approche de la prospection directe», aux pages 51 et 52.

soumis». Cela peut être le cas, par exemple, lorsque les employeurs doivent communiquer des données relatives aux rémunérations de leurs salariés à la sécurité sociale ou à l'administration fiscale, ou lorsque les institutions financières sont tenues de signaler certaines opérations suspectes aux autorités compétentes en vertu de règles visant à lutter contre le blanchiment d'argent. Il pourrait s'agir aussi d'une obligation à laquelle une autorité publique est soumise, puisque rien ne limite l'application de l'article 7, point c), au secteur privé ou public. Cette disposition s'appliquerait, par exemple, à la collecte de données par une autorité locale aux fins du traitement des amendes pour stationnement irrégulier.

L'article 7, point c), présente des similitudes avec l'article 7, point e), dans la mesure où une mission d'intérêt public repose souvent sur une disposition légale, ou en découle. Le champ d'application de l'article 7, point c), est néanmoins strictement délimité.

Pour que l'article 7, point c), puisse s'appliquer, l'obligation doit être imposée par la loi (et non, par exemple, par une cause contractuelle). La loi doit remplir toutes les conditions requises pour rendre l'obligation valable et contraignante, et doit aussi être conforme au droit applicable en matière de protection des données, notamment aux principes de nécessité, de proportionnalité[38] et de limitation de la finalité.

Il importe également de souligner que l'article 7, point c), se rapporte aux lois de l'Union européenne ou d'un État membre. Les obligations imposées par les lois de pays tiers (comme, par exemple, l'obligation de mettre en place des mécanismes de dénonciation des dysfonctionnements, instaurée en 2002 par la loi Sarbanes-Oxley aux États-Unis) ne relèvent pas de ce motif. Pour être valable, une obligation légale imposée par un pays tiers devrait être officiellement reconnue et intégrée dans l'ordre juridique de l'État membre concerné, par exemple sous la forme d'une convention internationale[39]. En revanche, la nécessité de satisfaire à une obligation étrangère peut représenter un intérêt légitime poursuivi par le responsable du traitement, mais uniquement sous réserve de respecter le critère de mise en balance de l'article 7, point f), et pour autant que des garanties adéquates aient été mises en place, comme celles approuvées par l'autorité compétente chargée de la protection des données.

Le responsable du traitement ne doit pas avoir le choix de se conformer ou non à l'obligation. Les engagements volontaires unilatéraux et les partenariats public-privé qui supposent le traitement de données au-delà de ce qui est requis par la loi n'entrent donc pas dans le champ d'application de l'article 7, point c). Par exemple, si un fournisseur de services internet décide – sans y être contraint par une obligation légale claire et précise – de surveiller ses utilisateurs afin de lutter contre le téléchargement illégal, l'article 7, point c), ne pourra pas être invoqué comme fondement juridique approprié à cet effet.

[38] Voir aussi l'avis 01/2014 du groupe de travail «Article 29» sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, adopté le 27. 2.2014 (WP 211).

[39] Voir, à ce propos, la section 4.2.2 de l'avis 10/2006 groupe de travail «Article 29» sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), adopté le 20.11.2006 (WP 128) et l'avis 1/2006 du groupe de travail «Article 29» relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, adopté le 1.2.2006 (WP 117).

De surcroît, l'obligation légale elle-même doit être suffisamment claire à propos du traitement de données à caractère personnel qu'elle requiert. En conséquence, l'article 7, point c), s'applique sur la base de dispositions juridiques mentionnant explicitement la nature et l'objet du traitement. Le responsable du traitement ne devrait pas avoir de marge d'appréciation injustifiée quant à la façon de se conformer à l'obligation légale.

La législation peut, dans certains cas, définir seulement un objectif général, tandis que des obligations plus spécifiques sont imposées à un niveau différent, par exemple, dans le droit dérivé ou dans une décision contraignante d'une autorité publique dans un cas concret. Cela peut aussi déboucher sur des obligations légales au sens de l'article 7, point c), pour autant que la nature et l'objet du traitement soient bien définis et qu'il existe une base juridique adéquate.

Il en va toutefois autrement si une autorité réglementaire formule uniquement des lignes directrices générales et énonce les conditions auxquelles elle pourrait envisager de faire usage de ses pouvoirs d'exécution (par exemple, des orientations réglementaires à l'intention des institutions financières portant sur certaines normes de vigilance). Dans de tels cas, les activités de traitement doivent être appréciées au regard de l'article 7, point f), et ne peuvent être considérées comme légitimes que sous réserve du respect du critère supplémentaire de mise en balance[40].

D'une manière générale, il convient de noter que certaines activités de traitement peuvent sembler relever, à peu de chose près, de l'article 7, point c), ou de l'article 7, point b), sans remplir pleinement les critères pour que ces motifs puissent s'appliquer. Cela ne veut pas dire qu'un tel traitement est toujours nécessairement illicite: il peut parfois être légitime, mais plutôt au titre de l'article 7, point f), sous réserve du respect du critère supplémentaire de mise en balance.

III.2.4. Intérêt vital

L'article 7, point d), constitue un fondement juridique dans les situations où le traitement «est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée». Ce libellé est différent des termes employés à l'article 8, paragraphe 2, point c), qui est plus précis et renvoie à des situations où «le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement».

Les deux dispositions paraissent néanmoins indiquer que ce fondement juridique devrait avoir une application limitée. Premièrement, l'expression «intérêt vital» semble limiter l'application de ce motif à des questions de vie ou de mort, ou, à tout le moins, à des menaces qui comportent un risque de blessure ou une autre atteinte à la santé de la personne concernée [ou aussi d'une autre personne, dans le cas de l'article 8, paragraphe 2, point c)].

Le considérant 31 confirme que l'objectif de ce fondement juridique est de «protéger un intérêt essentiel à la vie de la personne concernée». La directive n'indique cependant pas

[40] Des orientations émanant d'une autorité réglementaire peuvent néanmoins jouer un rôle dans l'appréciation de l'intérêt légitime poursuivi par le responsable du traitement [voir la section III.3.4, point a), notamment en page 40].

précisément si la menace doit être immédiate. Cela suscite des questions quant à la portée de la collecte de données, par exemple, à titre de mesure préventive ou à grande échelle, comme la collecte des données relatives aux passagers transportés par une compagnie aérienne en cas de risque d'épidémie ou d'incident de sûreté.

Le groupe de travail considère qu'il convient de donner une interprétation restrictive à cette disposition, conformément à l'esprit de l'article 8. Bien que l'article 7, point d), ne limite pas expressément l'utilisation de ce motif à des situations où le consentement ne peut servir de fondement juridique, pour les raisons mentionnées à l'article 8, paragraphe 2, point c), il est raisonnable de supposer que, lorsqu'il est possible et nécessaire de demander un consentement valable, il y a effectivement lieu d'obtenir ce consentement chaque fois que les conditions le permettent. Cette disposition verrait ainsi son application limitée à une analyse au cas par cas et elle ne pourrait normalement servir à légitimer ni la collecte massive de données à caractère personnel ni leur traitement. Au cas où cela s'avérerait nécessaire, les points c) ou e) de l'article 7 représenteraient des motifs plus appropriés pour justifier le traitement.

III.2.5. Mission d'intérêt public

L'article 7, point e), constitue un fondement juridique dans les situations où le traitement «est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées».

Il importe de noter que, tout comme l'article 7, point c), l'article 7, point e), se rapporte à l'intérêt public de l'Union européenne ou d'un État membre. De même, «l'autorité publique» désigne une autorité conférée par l'Union européenne ou par un État membre. Autrement dit, les missions menées dans l'intérêt public d'un pays tiers ou relevant de l'exercice d'une autorité publique conférée en vertu d'une législation étrangère n'entrent pas dans le champ d'application de cette disposition[41].

L'article 7, point e), recouvre deux situations et s'applique tant au secteur public qu'au secteur privé. Premièrement, il concerne des situations où le responsable du traitement est lui-même investi d'une autorité publique ou d'une mission d'intérêt public (sans nécessairement être lui aussi soumis à une obligation légale de traiter des données) et où le traitement est nécessaire à l'exercice de cette autorité ou de cette mission. Par exemple, une administration fiscale peut collecter et traiter la déclaration de revenus d'une personne afin d'établir et de vérifier le montant de l'impôt à payer. Ou une association professionnelle, comme un barreau d'avocats ou un ordre des médecins, investie de l'autorité publique requise, peut engager des procédures disciplinaires à l'encontre de certains de ses membres. Un autre exemple pourrait être celui d'une collectivité locale, comme une administration municipale, chargée de gérer une bibliothèque, une école ou une piscine.

Deuxièmement, l'article 7, point e), couvre aussi des situations où le responsable du traitement n'est pas investi d'une autorité publique, mais est invité à communiquer des données à un tiers investi d'une telle autorité. Par exemple, un agent d'un service public

[41] Voir la section 2.4 du document de travail du groupe de travail «Article 29» relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005 (WP 114), pour une interprétation similaire de la notion de «sauvegarde d'un intérêt public important» visée à l'article 26, paragraphe 1, point d).

compétent pour enquêter sur un crime peut demander au responsable du traitement sa coopération dans le cadre d'une enquête en cours, plutôt que de lui ordonner de se soumettre à une demande de coopération spécifique. L'article 7, point e), peut en outre couvrir des situations où le responsable du traitement communique des données, de manière proactive, à un tiers investi de cette autorité publique. Cela peut être le cas, par exemple, quand un responsable du traitement constate qu'une infraction pénale a été commise et transmet l'information aux services répressifs compétents de sa propre initiative.

À la différence de l'article 7, point c), il n'est pas nécessaire que le responsable du traitement soit soumis à une obligation légale. Pour reprendre l'exemple donné ci-dessus, un responsable du traitement qui remarquerait par hasard qu'une fraude ou un vol a été commis n'aurait peut-être pas l'obligation légale de le signaler à la police, mais il pourrait néanmoins, le cas échéant, le faire volontairement en vertu de l'article 7, point e).

Il faut cependant que le traitement soit «nécessaire à l'exécution d'une mission d'intérêt public», ou encore que le responsable du traitement ou le tiers auquel il communique les données soit investi d'une autorité publique et que le traitement des données soit nécessaire à l'exercice de cette autorité[42]. Il importe aussi de souligner que cette autorité publique ou cette mission d'intérêt public aura généralement été attribuée par une loi ou une autre règle de droit. Si le traitement suppose une ingérence dans la vie privée ou si le droit national l'exige par ailleurs afin de garantir la protection des personnes concernées, la base juridique encadrant le genre de traitement de données qui peut être autorisé devra être suffisamment précise et spécifique.

Ces situations deviennent de plus en plus courantes et se répandent aussi en dehors du secteur public, du fait de la tendance à sous-traiter des missions de l'administration à des entités du secteur privé. Cela peut être le cas, par exemple, pour les activités de traitement du secteur des transports ou de la santé (études épidémiologiques, recherches, etc.). Ce motif pourrait aussi être invoqué dans le cadre de l'action répressive, comme l'ont déjà montré les exemples ci-dessus. Cependant, la mesure dans laquelle une société privée peut être autorisée à coopérer avec les services répressifs, par exemple pour lutter contre la fraude ou le partage de contenu illégal sur l'internet, requiert une analyse au regard non seulement de l'article 7, mais aussi de l'article 6, afin de prendre en considération les exigences de limitation de la finalité, de licéité et de loyauté[43].

L'article 7, point e), a potentiellement un champ d'application très large, ce qui plaide en faveur d'une interprétation stricte et d'une définition précise, au cas par cas, de l'intérêt public en jeu et de l'autorité publique justifiant le traitement. Ce large champ d'application explique aussi pourquoi, comme dans le cas de l'article 7, point f), un droit d'opposition a été prévu à

[42] Autrement dit, dans ces cas, l'intérêt public des missions et la responsabilité correspondante subsisteront, même si l'exercice de la mission a été confié à d'autres entités, y compris dans le secteur privé.

[43] Voir, en ce sens, l'avis du groupe de travail «Article 29» sur SWIFT (cité précédemment, en note de bas de page 39), l'avis 4/2003 du groupe de travail «Article 29» sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers, adopté le 13.6.2003 (WP 78) et le document de travail sur les questions de protection des données liées aux droits de propriété intellectuelle, adopté le 18.1.2005 (WP 104).

l'article 14 quand le traitement est fondé sur l'article 7, point e)[44]. Des garanties et des mesures supplémentaires similaires peuvent donc s'appliquer dans les deux cas[45].

En ce sens, l'article 7, point e), présente des similitudes avec l'article 7, point f), et, dans certains contextes, pour les pouvoirs publics en particulier, le premier peut remplacer le second.

Pour apprécier la mesure dans laquelle ces dispositions s'appliquent aux organismes du secteur public, à la lumière notamment des propositions de changements à apporter au cadre juridique de la protection des données, il est utile de noter que texte actuel du règlement n° 45/2001[46], qui fixe les règles de protection des données applicables aux institutions et organes de l'Union européenne, ne contient aucune disposition comparable à l'article 7, point f).

Le considérant 27 de ce règlement prévoit néanmoins que «[l]e traitement de données à caractère personnel effectué pour l'exécution de *missions d'intérêt public* par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes». Cette disposition autorise donc le traitement des données pour un motif «d'intérêt public» au sens large dans des situations très variées, qui auraient pu, sinon, être couvertes par une disposition analogue à l'article 7, point f). La vidéosurveillance de locaux pour des raisons de sécurité, le contrôle électronique des échanges de courriels, ou les évaluations du personnel ne sont que quelques exemples des situations qui peuvent relever de cette disposition relative à «l'exécution de missions d'intérêt public» interprétée de manière large.

Dans une perspective d'avenir, il importe également de tenir compte du fait que le règlement proposé prévoit expressément, à l'article 6, paragraphe 1, point f), que les considérations relatives au motif de l'intérêt légitime «ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions». Si cette disposition est adoptée et interprétée au sens large, de façon à interdire totalement aux autorités publiques d'invoquer l'intérêt légitime comme fondement juridique, les motifs de la «mission d'intérêt public» et de «l'exercice de l'autorité publique» énoncés à l'article 7, point e), devraient recevoir une interprétation qui laisse aux pouvoirs publics une certaine latitude, pour au moins leur permettre d'assurer correctement leur gestion et leur fonctionnement, à l'instar de l'interprétation du règlement n° 45/2001 qui prévaut actuellement.

Une autre possibilité serait d'interpréter la dernière phrase de l'article 6, paragraphe 1, point f), du règlement proposé de façon à ne pas interdire totalement aux autorités publiques d'invoquer l'intérêt légitime comme fondement juridique. Dans ce cas, l'expression «traitement effectué par les autorités publiques dans l'exécution de leurs missions» figurant à l'article 6, paragraphe 1, point f), tel qu'il est proposé, devrait recevoir une interprétation restrictive, ne couvrant pas le traitement effectué aux fins d'assurer correctement la gestion et

[44] Comme indiqué précédemment, cette possibilité de s'opposer au traitement des données en vertu de l'article 7, point e), n'existe pas dans certains États membres (par exemple, en Suède).

[45] Comme on le verra plus loin, le projet de rapport de la commission LIBE recommandait d'autres garanties – en particulier, une transparence renforcée – dans le cas où l'article 7, point f), s'applique.

[46] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8, 12.1.2001, p. 1).

le fonctionnement de ces autorités publiques. De ce fait, il resterait possible d'invoquer le motif de l'intérêt légitime pour justifier le traitement nécessaire à la bonne gestion et au fonctionnement correct de ces pouvoirs publics.

III.3. Article 7, point f): intérêt légitime

L'article 7, point f)[47], impose un critère de mise en balance: l'intérêt légitime poursuivi par le responsable du traitement (ou par des tiers) doit être comparé avec l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le résultat de cette mise en balance détermine dans une large mesure si l'article 7, point f), peut servir de fondement juridique justifiant le traitement.

Il convient de préciser d'emblée que ce critère ne se borne pas à une simple mise en balance consistant à peser deux «poids» aisément quantifiables et comparables. Comme on le verra plus en détail dans la description présentée ci-après, cette mise en balance peut nécessiter une appréciation complexe de divers facteurs. Afin de mieux structurer et de simplifier l'évaluation, nous avons scindé le processus en plusieurs étapes pour garantir l'application effective du critère de mise en balance.

La section III.3.1 commence par examiner un plateau de la balance: ce qui constitue «l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées». Dans la section III.3.2, nous nous pencherons sur l'autre plateau de la balance, à savoir «l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, paragraphe 1».

Les sections III.3.3 et III.3.4 expliquent la manière dont le critère de mise en balance doit être appliqué. La section III.3.3 présente une introduction générale à l'aide de trois scénarios différents. Ensuite, la section III.3.4 expose les principales considérations dont il faut tenir compte pour appliquer le critère, et notamment les garanties et les mesures à prévoir par le responsable du traitement des données.

Enfin, dans les sections III.3.5 et III.3.6, nous examinerons aussi certains mécanismes particuliers tels que le principe de responsabilité, la transparence et le droit d'opposition, qui peuvent contribuer à assurer – et approfondir – une mise en balance correcte des divers intérêts en jeu.

III.3.1. Intérêt légitime poursuivi par le responsable du traitement (ou par des tiers)

La notion d'«intérêt»

La notion d'«intérêt» et celle de «finalité», mentionnée à l'article 6 de la directive, sont étroitement liées, mais néanmoins distinctes. En matière de protection des données, la «finalité» est la raison spécifique pour laquelle les données sont traitées: le but ou l'intention de leur traitement. L'intérêt, quant à lui, est l'enjeu plus large poursuivi par le responsable du traitement, ou le bénéfice qu'il tire – ou que la société pourrait tirer - du traitement.

[47] Pour le libellé complet de l'article 7, point f), voir la page 4 ci-dessus.

Par exemple, une entreprise peut avoir un *intérêt* à préserver la santé et la sécurité du personnel qui travaille dans sa centrale nucléaire. Pour ce faire, l'entreprise peut avoir comme *finalité* d'appliquer des procédures de contrôle d'accès spécifiques qui justifient le traitement de certaines données à caractère personnel afin de contribuer à protéger la santé et la sécurité des employés.

Un intérêt doit être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée. De plus, l'intérêt en jeu doit aussi être «poursuivi par le responsable du traitement». Cela suppose un intérêt réel et présent, qui correspond à des activités menées actuellement ou à des bénéfices escomptés dans un avenir très proche. Autrement dit, des intérêts trop vagues ou hypothétiques ne seront pas suffisants.

La nature de l'intérêt peut varier. Certains intérêts peuvent être impérieux et profitables à la société en général, comme l'intérêt de la presse à publier des informations sur des faits de corruption dans l'administration ou l'intérêt d'effectuer des recherches scientifiques (sous réserve de garanties appropriées). D'autres intérêts peuvent être moins pressants pour l'ensemble de la société ou, en tout cas, leur poursuite peut avoir une incidence plus mitigée ou controversée sur la collectivité. Cela peut s'appliquer, par exemple, à l'intérêt économique d'une entreprise à en savoir le plus possible sur ses clients potentiels afin de mieux cibler la publicité pour ses produits ou services.

Qu'est-ce qui rend un intérêt «légitime» ou «illégitime»?

Cette question vise à déterminer le seuil de ce qui constitue un intérêt légitime. Si l'intérêt poursuivi par le responsable du traitement des données est illégitime, le critère de mise en balance n'aura pas à être appliqué, puisque le seuil initial permettant d'invoquer l'article 7, point f), n'aura pas été atteint.

Le groupe de travail considère que la notion d'intérêt légitime pourrait inclure des intérêts très variés, qu'ils soient futiles ou incontestables, évidents ou plus controversés. C'est donc dans un deuxième temps, lorsqu'il s'agira de mettre en balance ces intérêts avec les intérêts et droits fondamentaux des personnes concernées, qu'il conviendra d'adopter une approche plus restreinte et de procéder à une analyse plus approfondie.

La liste qui suit énumère de façon non exhaustive certains des contextes où la question de l'intérêt légitime au sens de l'article 7, point f), est le plus communément susceptible de se poser. Elle est présentée ici sans préjuger si l'intérêt poursuivi par le responsable du traitement prévaudra en définitive sur l'intérêt et les droits des personnes concernées après la mise en balance.

- Exercice du droit à la liberté d'expression ou d'information, notamment dans les médias et dans les arts;
- prospection directe conventionnelle et autres formes de prospection commerciale ou de publicité;
- messages non commerciaux non sollicités, notamment à des fins de campagne politique ou de collecte de fonds pour des actions caritatives;
- exécution de demandes en justice, y compris le recouvrement de créances via des procédures extrajudiciaires;

- prévention de la fraude, de l'utilisation abusive de services, ou du blanchiment d'argent;
- surveillance du personnel à des fins de sécurité ou de gestion;
- mécanismes de dénonciation des dysfonctionnements;
- sécurité physique, sécurité des systèmes et réseaux informatiques;
- traitement à finalité historique, scientifique ou statistique;
- traitement à des fins de recherche (y compris la recherche commerciale).

En conséquence, un intérêt peut être considéré comme légitime dès lors que le responsable du traitement est en mesure de poursuivre cet intérêt dans le respect de la législation sur la protection des données et d'autres législations. Autrement dit, un intérêt légitime doit être «acceptable au regard du droit»[48].

Pour être pertinent au regard de l'article 7, point f), un «intérêt légitime» doit donc:

- être licite (c'est-à-dire conforme au droit en vigueur dans l'Union et dans le pays concerné);
- être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment précis);
- constituer un intérêt réel et présent (c'est-à-dire non hypothétique).

Le fait que le responsable du traitement poursuive un tel intérêt légitime en traitant certaines données ne signifie pas qu'il puisse nécessairement invoquer l'article 7, point f), comme fondement juridique justifiant le traitement. La légitimité de l'intérêt poursuivi n'est qu'un point de départ, un des éléments qui doivent être analysés en vertu de l'article 7, point f). La possibilité d'invoquer cette disposition dépendra du résultat de la mise en balance qui suit.

À titre d'illustration: des responsables du traitement peuvent avoir un intérêt légitime à connaître les préférences de leurs clients pour être en mesure de mieux personnaliser leurs offres et, en fin de compte, de proposer des produits et des services qui correspondent mieux aux besoins et aux désirs des clients. Dans cette perspective, l'article 7, point f), peut constituer un fondement juridique approprié pour certains types d'activités de prospection, en ligne ou hors ligne, pour autant qu'il existe des garanties appropriées [incluant, entre autres, un mécanisme fonctionnel permettant de s'opposer à ce traitement conformément à

[48] Les observations concernant la nature de la «légitimité» formulées à la section III.1.3 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus) s'appliquent aussi ici, mutatis mutandis. Comme il est indiqué aux pages 19 et 20 de cet avis, la notion de «droit» est utilisée ici dans son sens le plus large. Cela inclut d'autres législations applicables, par exemple en matière d'emploi, de contrats, ou de protection des consommateurs. De plus, la notion de droit «inclut toutes les formes de droit écrit et coutumier, le droit primaire et le droit dérivé, les arrêtés municipaux, les précédents judiciaires, les principes constitutionnels, les droits fondamentaux, d'autres principes juridiques, ainsi que la jurisprudence, tel que ce "droit" serait interprété et pris en compte par des juridictions compétentes. Dans les limites du droit, d'autres éléments comme les coutumes, les codes de conduite, les codes de déontologie, les accords contractuels, ainsi que les circonstances et le contexte général peuvent aussi être pris en considération pour déterminer si une finalité particulière est légitime. Cela peut comprendre la nature de la relation sous-jacente entre le responsable du traitement et les personnes concernées, qu'elle soit commerciale ou autre». En outre, ce qui peut être considéré comme un intérêt légitime «peut aussi changer au fil du temps, en fonction des progrès scientifiques et technologiques, et des évolutions de la société et des attitudes culturelles».

l'article 14, paragraphe b), comme on le verra à la section III.3.6, *Le droit d'opposition et au-delà*].

Cela ne signifie pas pour autant que les responsables du traitement pourraient invoquer l'article 7, point f), pour surveiller indûment les activités en ligne ou hors ligne de leurs clients, pour compiler d'importants volumes de données à leur propos en provenance de différentes sources, collectées à l'origine dans d'autres contextes et à des fins différentes, et pour créer – mais aussi, par exemple, échanger en passant par des courtiers en informations – des profils complexes concernant la personnalité et les préférences des clients, sans les en informer ni mettre à leur disposition un mécanisme fonctionnel permettant d'exprimer leur opposition, pour ne rien dire de leur consentement éclairé. Une telle activité de profilage risque de constituer une violation grave de la vie privée du client et, dans ce cas, l'intérêt et les droits de la personne concernée prévaudraient sur l'intérêt poursuivi par le responsable du traitement[49].

Pour donner un autre exemple, dans son avis sur SWIFT[50], le groupe de travail concluait, tout en reconnaissant l'intérêt légitime de la société à se conformer aux sommations du droit des États-Unis pour éviter le risque d'être sanctionnée par les autorités américaines, que l'article 7, point f), ne pouvait pas être invoqué. Le groupe de travail considérait notamment qu'en raison des conséquences considérables pour les particuliers du traitement de données effectué d'une manière «cachée, systématique, massive et de longue durée», «les intérêts des nombreuses personnes concernées sur le plan des libertés et des droits fondamentaux prévalent [contre] ceux de SWIFT à ne pas être sanctionnée par les États-Unis pour non-soumission éventuelle à une sommation».

Comme on le verra plus tard, si l'intérêt poursuivi par le responsable du traitement n'est pas impérieux, l'intérêt et les droits de la personne concernée ont plus de chances de prévaloir contre l'intérêt légitime – mais moins important – du responsable du traitement. Il ne s'ensuit pas, cependant, que des intérêts moins impérieux poursuivis par le responsable du traitement ne puissent pas, parfois, prévaloir contre l'intérêt et les droits des personnes concernées: cela arrive généralement quand les conséquences du traitement pour les personnes concernées sont aussi moins importantes.

L'intérêt légitime dans le secteur public

Le texte actuel de la directive n'exclut pas expressément que les responsables du traitement qui sont des autorités publiques puissent se servir de l'article 7, point f), comme fondement juridique pour traiter des données[51].

[49] La question des techniques de traçage et le rôle du consentement exigé par l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» seront discutés séparément. Voir la section III.3.6, point b), sous l'intitulé: «Illustration: l'évolution de l'approche de la prospection directe».

[50] Voir la section 4.2.3 de l'avis déjà cité en note de bas de page 39. L'intérêt légitime poursuivi par le responsable du traitement dans cette affaire était aussi lié à l'intérêt public d'un pays tiers, qui ne saurait relever de la directive 95/46/CE.

[51] À l'origine, la première proposition de directive de la Commission couvrait séparément le traitement des données dans le secteur privé et les activités de traitement dans le secteur public. Cette distinction formelle entre les règles applicables au secteur public et au secteur privé a été abandonnée dans la proposition modifiée. Cela aurait aussi pu entraîner des divergences d'interprétation et de mise en œuvre par les divers États membres.

Cependant, la proposition de règlement[52] exclut cette possibilité pour le «traitement effectué par les autorités publiques dans l'exécution de leurs missions».

Le changement législatif proposé fait ressortir l'importance du principe selon lequel, en règle générale, les autorités publiques ne devraient traiter des données à caractère personnel dans l'exécution de leurs missions que si elles y sont dûment autorisées par la loi. Le respect de ce principe est particulièrement important – et clairement requis par la jurisprudence de la Cour européenne des droits de l'homme – dans les cas où la vie privée des personnes concernées est en jeu et où les activités de l'autorité publique constitueraient une ingérence dans cette vie privée.

Une autorisation suffisamment *détaillée et précise* prévue par la loi est donc exigée – dans la directive actuelle également – lorsque le traitement par les autorités publiques suppose une ingérence dans la vie privée des personnes concernées. Cela peut prendre la forme d'une obligation légale spécifique de traiter des données, conformément à l'article 7, point c), ou d'une autorisation spécifique (sans qu'il s'agisse nécessairement d'une obligation) de traiter des données, dans le respect des exigences de l'article 7, point e) ou f)[53].

L'intérêt légitime des tiers

Le texte actuel de la directive ne mentionne pas seulement «l'intérêt légitime poursuivi par le responsable du traitement» mais autorise aussi l'invocation de l'article 7, point f), quand l'intérêt légitime est poursuivi par «les tiers auxquels les données sont communiquées»[54]. Les exemples suivants illustrent certaines des situations où cette disposition peut s'appliquer.

Publication de données à des fins de transparence et de responsabilité. Un contexte important où l'article 7, point f), peut être pertinent est celui où la publication de données vise à assurer la transparence et la responsabilité (par exemple, les salaires des dirigeants d'une entreprise). Dans ce cas, on peut considérer que la divulgation publique est effectuée principalement non pas dans l'intérêt du responsable du traitement qui publie les données, mais dans celui d'autres parties prenantes, comme les salariés, la presse ou l'opinion publique, à qui les données sont communiquées.

Dans une perspective de protection des données et de respect de la vie privée, et afin de garantir la sécurité juridique, en général, il est souhaitable que les données à caractère personnel soient rendues publiques en vertu d'une loi qui l'autorise et, s'il y a lieu, qui

[52] Voir l'article 6, paragraphe 1, point f), de la proposition de règlement.

[53] À cet égard, voir aussi la section III.2.5 ci-dessus à propos des missions d'intérêt public (pages 23 à 25) ainsi que les considérations présentées ci-après sous l'intitulé *L'intérêt légitime des tiers* (pages 30 à 32). Voir aussi les réflexions sur les limites de «l'application du droit par la sphère privée», en page 39 sous l'intitulé «Intérêt public/intérêt de la collectivité». Dans toutes ces situations, il importe particulièrement de veiller au respect absolu des limites définies par l'article 7, point f), et aussi par l'article 7, point e).

[54] La proposition de règlement entend restreindre l'utilisation de ce motif aux «intérêts légitimes poursuivis par un responsable du traitement». Il n'apparaît pas clairement, à la lecture du texte seul, si le libellé proposé correspond uniquement à une volonté de simplification du texte ou si son intention est d'exclure les situations où un responsable du traitement pourrait communiquer des données dans l'intérêt légitime poursuivi par d'autres. Ce texte n'est cependant pas définitif. L'intérêt des tiers a, par exemple, été réintroduit dans le rapport final de la commission LIBE à l'occasion du vote des amendements de compromis par cette commission du Parlement européen le 21 octobre 2013. Voir l'amendement 100 sur l'article 6. Le groupe de travail est favorable à la réintroduction de l'intérêt des tiers dans la proposition, étant donné que son utilisation peut demeurer appropriée dans certaines situations, notamment celles décrites ci-après.

spécifie clairement les données à publier, la finalité de la publication et toutes les garanties nécessaires[55]. Il s'ensuit également qu'il peut être préférable que l'article 7, point c), plutôt que l'article 7, point f), serve de fondement juridique quand des données à caractère personnel sont divulguées à des fins de transparence et de responsabilité[56].

Cependant, en l'absence d'une obligation légale expresse ou de la permission de publier des données, il serait néanmoins possible de communiquer des données à caractère personnel à des parties intéressées. Dans des circonstances appropriées, il serait aussi possible de publier des données à caractère personnel à des fins de transparence et de responsabilité.

Dans les deux cas – c'est-à-dire indépendamment du fait que les données à caractère personnel soient divulguées en vertu d'une loi l'autorisant ou non – la divulgation dépend directement du résultat de la mise en balance prévue à l'article 7, point f), et de la mise en œuvre de garanties et de mesures appropriées[57].

En outre, l'utilisation ultérieure, dans un souci de plus grande transparence, de données à caractère personnel déjà publiées (par exemple, la republication des données par la presse, ou la diffusion ultérieure d'un ensemble de données publiées initialement, d'une manière plus innovante ou conviviale par une ONG), peut aussi être souhaitable. La possibilité ou non de republier et de réutiliser les données dépendra également du résultat de la mise en balance, qui devrait tenir compte, en autres, de la nature des informations et des conséquences pour les particuliers de la republication ou de la réutilisation[58].

Recherche historique ou autres formes de recherche scientifique. Un autre contexte important dans lequel la divulgation dans l'intérêt légitime poursuivi par des tiers peut être pertinente se rapporte à la recherche historique ou à d'autres formes de recherche scientifique, en particulier lorsque ces travaux nécessitent un accès à certaines bases de données. La directive reconnaît expressément ces activités, sous réserve de garanties et de mesures appropriées[59],

[55] Cette recommandation de bonnes pratiques ne devrait pas remettre en cause les dispositions nationales en matière de transparence et d'accès public aux documents.

[56] En effet, dans certains États membres, il faut respecter des règles différentes pour le traitement effectué par des parties du secteur public ou privé. Par exemple, selon le code italien de la protection des données, la diffusion de données à caractère personnel par un organisme public n'est autorisée que si elle est prévue par une loi ou un règlement (article 19.3).

[57] Comme l'explique l'avis 06/2013 du groupe de travail «Article 29» sur les données ouvertes (voir page 9 de cet avis, cité en note de bas de page 88 ci-après), «la législation nationale doit respecter l'article 8 de la Convention européenne des droits de l'homme (CEDH) et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne («Charte de l'UE»). Cela implique, comme l'a déclaré la Cour de justice de l'UE dans ses arrêts Österreichischer Rundfunk et Schecke, qu'il faut établir que la divulgation «est nécessaire et proportionnée au but légitime recherché». Voir l'arrêt de la Cour du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01, Rundfunk, et l'arrêt de la Cour du 9 novembre 2010, dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke.

[58] La limitation de la finalité constitue également une considération importante à cet égard. En page 22 de son avis 06/2013 sur les données ouvertes (cité en note de bas de page 88 ci-après), le groupe de travail recommande «que toute loi qui demande un accès public à des données énonce clairement les finalités de la divulgation des données à caractère personnel. Si ce n'est pas le cas, ou si seuls des termes généraux et vagues sont employés, la sécurité juridique et la prévisibilité en souffriront. En particulier, pour toute demande de réutilisation, l'organisme du secteur public et les réutilisateurs potentiels éprouveront de grandes difficultés à déterminer la finalité première de la publication et, ensuite, les autres finalités qui seraient compatibles avec cette finalité. Comme cela a été dit précédemment, même si les données à caractère personnel sont publiées sur l'internet, cela n'implique pas qu'elles peuvent faire l'objet d'un traitement ultérieur pour toute autre finalité.»

[59] Voir, par exemple, l'article 6, paragraphe 1, points b) et e).

mais il ne faut pas oublier que le fondement légitime de ces activités résidera souvent dans une utilisation mûrement réfléchie de l'article 7, point f)[60].

Intérêt général ou intérêt d'un tiers. Enfin, l'intérêt légitime des tiers peut aussi être pertinent à d'autres égards. C'est le cas lorsqu'un responsable du traitement – parfois encouragé par les autorités publiques – poursuit un intérêt qui correspond à l'intérêt général ou à l'intérêt d'un tiers. Il peut s'agir notamment de situations où le responsable du traitement va plus loin que les obligations légales spécifiques qui lui sont imposées par des lois ou des réglementations afin d'aider les services répressifs ou des acteurs privés dans leur lutte contre des activités illégales, comme le blanchiment d'argent, la séduction malintentionnée de mineurs ou le partage illégal de fichiers en ligne. Dans ces situations, cependant, il importe particulièrement de veiller à ce que les limites prévues par l'article 7, point f), soient pleinement respectées[61].

Le traitement doit être nécessaire à la/aux finalité(s) visée(s)

Enfin, le traitement des données à caractère personnel doit aussi être «nécessaire à la réalisation de l'intérêt légitime» poursuivi par le responsable du traitement ou – en cas de communication des données – par le tiers. Cette condition complète l'exigence de nécessité au titre de l'article 6 et suppose l'existence d'un lien entre le traitement et l'intérêt poursuivi. Cette exigence de «nécessité» s'applique dans toutes les situations mentionnées à l'article 7, points b) à f), mais elle est particulièrement pertinente dans le cas du point f), afin de garantir que le traitement des données fondé sur l'intérêt légitime ne débouche pas sur une interprétation trop large de la nécessité de traiter des données. Comme dans les autres cas, cela signifie qu'il y a lieu d'examiner s'il existe d'autres moyens plus respectueux de la vie privée susceptibles de servir la même finalité.

III.3.2. L'intérêt ou les droits de la personne concernée

L'intérêt ou les droits (et non, comme il est écrit dans la version anglaise, «interests for rights»)

Le texte anglais de l'article 7, point f), de la directive mentionne «the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)».

Le groupe de travail a cependant constaté, en comparant les différentes versions linguistiques de la directive, que l'expression «interests for» a été traduite avec le sens de «interests or» dans d'autres langues importantes utilisées lorsque le texte a été négocié[62].

[60] Comme l'explique l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus), l'utilisation ultérieure de données à des fins secondaires devrait être subordonnée à une double condition. Premièrement, il convient de veiller à ce que les données servent à des finalités compatibles. Deuxièmement, il y a lieu de vérifier si le traitement est fondé sur une base juridique appropriée au titre de l'article 7.

[61] Voir à cet égard, par exemple, le document de travail sur les questions de protection des données liées aux droits de propriété intellectuelle, adopté le 18.1.2005 (WP 104).

[62] Par exemple, «l'intérêt ou les droits et libertés fondamentaux de la personne concernée» en français, «l'interesse o i diritti e le libertà fondamentali della persona interessata» en italien; «das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person», en allemand.

Une analyse plus approfondie donne à penser que le libellé anglais de la directive est simplement le résultat d'une faute de frappe: «or» a été erronément dactylographié «for»[63]. Le texte anglais correct devrait donc être: «interests or fundamental rights and freedoms».

Il convient de donner une interprétation large aux notions d'«intérêt» et de «droits»

La mention de «l'intérêt ou les droits et libertés fondamentaux» a une incidence directe sur le champ d'application de la disposition. Elle accorde davantage de protection à la personne concernée, c'est-à-dire qu'elle requiert que l'«intérêt» des personnes concernées soit lui aussi pris en considération, et non pas seulement ses droits et libertés fondamentaux. Il n'y a cependant aucune raison de supposer que la restriction de l'article 7, point f), aux droits fondamentaux «qui appellent une protection au titre de l'article 1er paragraphe 1» – et donc la référence explicite à l'objet de la directive[64] – ne s'appliquerait pas aussi au terme «intérêt». Le message sans équivoque est néanmoins que tous les intérêts pertinents de la personne concernée devraient être pris en compte.

Cette interprétation du texte paraît logique, non seulement du point de vue grammatical, mais aussi compte tenu de la large interprétation de la notion d'«intérêt légitime» du responsable du traitement. Si le responsable du traitement – ou le tiers en cas de communication des données – peut poursuivre n'importe quel intérêt, pour autant qu'il ne soit pas illégitime, la personne concernée devrait aussi pouvoir s'attendre à ce que ses intérêts de toutes sortes soient pris en considération et mis en balance avec ceux du responsable du traitement, pour autant qu'ils soient pertinents dans le champ d'application de la directive.

En ces temps où croît le déséquilibre du «pouvoir de l'information», à l'heure où administrations et entreprises amassent des volumes sans précédent de données concernant les individus et se donnent de plus en plus les moyens de constituer des profils détaillés qui prédiront leurs comportements (au risque de renforcer encore le déséquilibre informationnel et d'amoindrir l'autonomie des citoyens), il est plus crucial que jamais de protéger l'intérêt des personnes à préserver leur vie privée et leur autonomie.

Enfin, il importe de relever qu'à la différence de l'«intérêt» du responsable du traitement, l'«intérêt» des personnes concernées n'est pas suivi ici de l'adjectif «légitime». Cela suppose que la protection de l'intérêt et des droits des individus a une portée plus vaste. Même les personnes qui se livrent à des activités illégales ne devraient pas faire l'objet d'une ingérence disproportionnée dans l'exercice de leurs droits et de leurs intérêts[65]. Par exemple, un individu

[63] Le groupe de travail «Article 29» observe que, pour être correcte du point de vue grammatical, la version anglaise aurait dû être «interests in» plutôt que «interests for», si telle avait été la signification voulue. De plus, l'expression «interests for» ou «interest in» paraît être redondante, puisque, si le sens avait été celui-là, la mention «fundamental rights and freedoms» aurait normalement suffi. L'interprétation selon laquelle il s'agit d'une faute de frappe est aussi confirmée par le fait que la position commune (CE) n° 1/95 adoptée par le Conseil le 20 février 1995 mentionne aussi «interests or fundamental rights and freedoms». Enfin, le groupe de travail «Article 29» note que la Commission entendait corriger cette faute de frappe dans le règlement proposé: l'article 6, paragraphe 1, point f), mentionne «the interests or fundamental rights and freedoms of the data subject which require protection of personal data» et non «interests for».

[64] Voir l'article 1er, paragraphe 1: «Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.»

[65] Bien sûr, l'une des conséquences de la criminalité pourrait être la collecte et l'éventuelle publication de données à caractère personnel concernant les criminels et les suspects, sous réserve cependant de garanties et de conditions strictes.

qui peut avoir commis un vol dans un supermarché pourrait encore voir son intérêt prévaloir contre la publication par le propriétaire du magasin de sa photo et de son adresse privée sur les murs du supermarché ou et/ou sur l'internet.

III.3.3. Introduction à l'application du critère de mise en balance

Il est utile d'imaginer que l'intérêt légitime poursuivi par le responsable du traitement et les incidences sur l'intérêt et les droits de la personne concernée se présentent sous la forme d'un spectre. L'intérêt légitime peut être, selon les cas, minime, relativement important ou impérieux. De même, les incidences sur l'intérêt et les droits des personnes concernées peuvent présenter plus ou moins de gravité et peuvent être anodines ou très préoccupantes.

L'intérêt légitime poursuivi par le responsable du traitement, quand il est peu important, ne prévaut généralement sur l'intérêt et les droits des personnes concernées que dans les cas où les incidences sont encore plus insignifiantes. D'un autre côté, un intérêt légitime impérieux peut justifier, dans certains cas et sous réserve de garanties et de mesures adéquates, une ingérence même grave dans la vie privée ou d'autres conséquences importantes pour l'intérêt ou les droits des personnes concernées[66].

Il importe ici de souligner le rôle essentiel que les garanties peuvent jouer[67] pour réduire les incidences injustifiées sur les personnes concernées et, partant, modifier l'équilibre des droits et des intérêts, au point que ceux de ces personnes ne prévalent plus sur l'intérêt légitime poursuivi par le responsable du traitement des données. Le recours à des garanties ne suffit bien sûr pas à justifier, à lui seul, n'importe quel traitement dans toutes les situations envisageables. Il faut en outre que les garanties en question soient adéquates et suffisantes, et qu'elles réduisent indubitablement et sensiblement les incidences sur les personnes concernées.

---

[66] Voir, à titre d'illustration, le raisonnement suivi par le groupe de travail «Article 29» dans plusieurs avis et documents de travail:
- Avis 4/2006 sur la *Notice of Proposed Rulemaking* (notification de proposition de règlement) du US Department of Health and Human Services, du 20 novembre 2005, relative au contrôle des maladies contagieuses et à la collecte d'informations sur les passagers (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71), adopté le 14.6.2006 (WP 121, en anglais), qui traite de graves menaces spécifiques pour la santé publique.
- Avis 1/2006 sur les mécanismes de dénonciation des dysfonctionnements (cité précédemment en note de bas page note 39), qui fait intervenir la gravité d'une infraction alléguée parmi les éléments du critère de mise en balance.
- Document concernant la surveillance des communications électroniques sur le lieu de travail, adopté le 29.5.2002 (WP 55), qui met en balance le droit de l'employeur à gérer efficacement son entreprise avec la dignité humaine du travailleur, ainsi qu'avec le secret de la correspondance.

[67] Les garanties peuvent inclure, notamment, des limitations strictes du volume de données collectées, la suppression immédiate des données après utilisation, des mesures techniques et organisationnelles visant à garantir une séparation fonctionnelle, l'utilisation appropriée de techniques d'anonymisation, l'agrégation des données, et des technologies renforçant la protection de la vie privée, mais aussi plus de transparence, de responsabilité et la possibilité de s'opposer au traitement. Voir aussi la section III.3.4, point d) et plus bas.

Scénarios de présentation

Avant de passer aux orientations sur les modalités d'application du critère de mise en balance, les trois scénarios de présentation suivants peuvent illustrer, en guise d'introduction, comment se présente l'équilibre des intérêts et des droits dans la réalité. Les trois exemples reposent sur un scénario simple et anodin, qui commence avec une offre promotionnelle pour la livraison à domicile de plats italiens. Les exemples introduisent progressivement de nouveaux éléments qui montrent comment la balance se met à pencher d'un côté, tandis que l'incidence sur les personnes concernées augmente.

Scénario 1: offre spéciale d'une chaîne de pizzérias

Claudia commande une pizza via une application mobile de son smartphone, mais ne s'oppose pas à l'envoi d'offres commerciales sur le site internet. Son adresse et les informations de sa carte de crédit sont enregistrées en vue de la livraison. Quelques jours plus tard, Claudia reçoit des coupons de réduction pour des produits similaires de la chaîne de pizzérias dans la boîte à lettres de son domicile.

Analyse succincte: la chaîne de pizzérias a un intérêt légitime, mais pas particulièrement impérieux, à chercher à vendre davantage de ses produits à ses clients. D'un autre côté, il ne semble pas y avoir d'ingérence importante dans la vie privée de Claudia, ni aucune incidence injustifiée sur son intérêt et ses droits. Les données et le contexte sont relativement anodins (consommation de pizzas). La chaîne de pizzérias a mis en place certaines garanties: les informations utilisées sont relativement limitées (coordonnées de contact) et les coupons sont envoyés par courrier traditionnel. De plus, une possibilité de refuser l'envoi de publicités est prévue sur le site internet et est relativement facile à utiliser.

Tout bien pesé, et compte tenu des garanties et mesures en place (dont un outil permettant facilement de s'opposer au traitement), l'intérêt et les droits de la personne concernée ne semblent pas prévaloir sur l'intérêt légitime de la chaîne de pizzérias à procéder à ce traitement de données minimal.

Scénario 2: publicité ciblée pour la même offre promotionnelle

Le contexte est le même, mais cette fois la chaîne de pizzérias conserve non seulement l'adresse et les informations de la carte de crédit de Claudia, mais aussi son historique de commandes récent (au cours des trois dernières années). En outre, l'historique des achats est combiné avec des données provenant du supermarché où Claudia fait ses courses en ligne, qui est géré par la même société que celle qui exploite la chaîne de pizzérias. Claudia se voit proposer par la chaîne de pizzérias des offres promotionnelles et des publicités ciblées fondées sur son historique de commandes pour les deux services différents. Elle reçoit les offres promotionnelles en ligne et hors ligne, par courrier ordinaire, par courrier électronique, et par l'affichage des offres sur le site internet de la société, ainsi que sur le site de plusieurs partenaires commerciaux (quand elle accède à ces sites sur son ordinateur ou via son téléphone mobile). Son historique de navigation est aussi suivi. Ses données de localisation sont tracées via son téléphone mobile. Un logiciel analyse les données et prédits ses préférences, ainsi que les moments et les lieux où elle sera le plus encline à effectuer un achat plus important, disposée à payer un prix plus élevé, susceptible d'être influencée par un taux

de réduction particulier, ou quand elle a le plus envie de ses desserts ou plats préparés favoris[68]. Claudia est fortement agacée par les publicités qui s'affichent constamment sur son téléphone mobile quand elle vérifie l'horaire des bus pour rentrer chez elle, avec les dernières offres de plats à emporter auxquelles elle tente de résister. Elle n'a pas réussi à trouver des informations conviviales ou un moyen simple pour faire cesser ces publicités, bien que la société prétende avoir mis en place un mécanisme d'opposition au traitement des données qui couvre tout le secteur. Elle a aussi été surprise de constater qu'après avoir déménagé dans un quartier moins aisé, elle ne recevait plus d'offres promotionnelles. Sa facture mensuelle pour les achats d'alimentation a de ce fait augmenté d'environ 10 %. Un ami plus versé dans les nouvelles technologies lui a fait lire certaines hypothèses publiées sur un blog, selon lesquelles le supermarché facturerait plus cher les commandes provenant de «mauvais quartiers», en raison des risques statistiquement plus élevés de fraude à la carte de crédit. La société se refuse à tout commentaire et se retranche derrière la confidentialité de sa politique d'offres promotionnelles et le caractère propriétaire de l'algorithme utilisé pour fixer les prix.

Analyse succincte: les données et le contexte demeurent relativement bénins. Toutefois l'ampleur de la collecte de données et les méthodes utilisées pour influencer Claudia (y compris diverses techniques de traçage, la prévision des moments et des lieux propices aux envies de nourriture et le fait que Claudia est alors plus vulnérable et risque de céder à la tentation) sont des facteurs à prendre en considération pour apprécier l'impact du traitement. Le manque de transparence quant à la logique du traitement de données effectué par la société, qui peut avoir entraîné une discrimination de fait en matière de prix sur la base du lieu où une commande est passée, et les conséquences financières potentiellement importantes pour les clients font, en fin de compte, pencher la balance, même dans le contexte assez anodin des courses alimentaires et des repas à emporter. Au lieu de donner simplement la possibilité de refuser ce type de profilage et de publicité ciblée, un consentement informé serait nécessaire, conformément à l'article 7, point a), de la directive 95/46/CE, mais aussi à l'article 5, paragraphe 3) de la directive «vie privée et communications électroniques». En conséquence, l'article 7, point f), ne devrait pas pouvoir être invoqué comme fondement juridique justifiant le traitement.

Scénario 3: utilisation des commandes de denrées alimentaires pour adapter les primes d'assurance santé

Les habitudes de consommation de Claudia, y compris le moment et la nature de ses commandes de nourriture, sont vendues par la chaîne de pizzérias à une compagnie d'assurances, qui s'en sert pour ajuster ses primes d'assurance santé.

Analyse succincte: la compagnie d'assurance santé peut avoir un intérêt légitime – dans la mesure où la législation applicable l'y autorise – à évaluer les risques sanitaires auxquels s'exposent ses assurés et à leur faire payer des primes variables selon les différents risques. Cependant, la façon dont les données sont collectées et l'ampleur même de la collecte de

[68] Voir, par exemple, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *«Des recherches récentes indiquent que la volonté est une ressource limitée que l'on peut épuiser ou reconstituer au fil du temps. Imaginez que la crainte de l'obésité incite une consommatrice à essayer de résister à son penchant pour la malbouffe. Il y aura forcément des moments et des endroits où elle en sera incapable. À l'aide d'un volume considérable de données, les publicitaires peuvent parvenir à comprendre exactement quand et comment approcher cette consommatrice lorsqu'elle est le plus vulnérable – surtout dans un monde constamment connecté où même nos appareils électroménagers sont capables de nous baratiner.»*

données sont excessives. Une personne raisonnable se trouvant dans la situation de Claudia ne s'attendrait probablement pas à ce que des informations sur sa consommation de pizzas puissent servir à calculer ses primes d'assurance santé.

En plus du caractère excessif du profilage et de la possibilité de suppositions inexactes (les pizzas pourraient avoir été commandées pour quelqu'un d'autre), le fait de déduire des données sensibles (risque sanitaire) à partir de données apparemment anodines (commande de repas à domicile) contribue à faire pencher la balance en faveur de l'intérêt et des droits de la personne concernée. Enfin, le traitement a aussi un impact financier considérable sur elle.

Tout bien pesé, dans ce cas spécifique, l'intérêt et les droits de la personne concernée prévalent sur l'intérêt légitime de la compagnie d'assurance santé. En conséquence, l'article 7, point f), ne devrait pas pouvoir être invoqué comme fondement juridique justifiant le traitement. Il est par ailleurs douteux que l'article 7, point a), puisse être utilisé, au regard de l'ampleur excessive de la collecte de données et peut-être aussi d'autres restrictions spécifiques imposées par le droit national.

Les scénarios présentés ci-dessus et la possibilité d'introduire des variantes comportant d'autres éléments soulignent la nécessité de disposer d'un nombre limité de facteurs-clés qui aideront à focaliser le travail d'appréciation, ainsi que d'une approche pragmatique permettant d'employer des hypothèses pratiques («méthode empirique») fondées principalement sur ce qu'une personne raisonnable jugerait acceptable selon les circonstances («attentes raisonnables») et compte tenu des conséquences de l'activité de traitement des données pour les personnes concernées («incidence»).

III.3.4. Facteurs-clés à prendre en considération pour appliquer le critère de mise en balance

Les États membres ont défini plusieurs facteurs utiles à prendre en considération pour appliquer le critère de mise en balance. La présente section examine ces facteurs dans quatre rubriques principales: a) appréciation de l'intérêt légitime du responsable du traitement, b) incidence sur les personnes concernées, c) bilan provisoire et d) garanties supplémentaires mises en place par le responsable du traitement afin de prévenir toute incidence injustifiée sur les personnes concernées[69].

Pour appliquer le critère de mise en balance, il importe, tout d'abord, d'examiner la nature et la source de l'intérêt légitime, d'une part, et l'incidence sur les personnes concernées, d'autre part. Cette appréciation devrait déjà tenir compte des mesures que le responsable du traitement prévoit d'adopter pour se conformer à la directive (afin, par exemple, de respecter la limitation de la finalité et la proportionnalité, comme l'exige l'article 6, ou d'informer les personnes concernées, conformément aux articles 10 et 11).

Après une analyse et un examen attentif de tous les aspects du problème, un bilan provisoire pourra être établi. Si le résultat de l'évaluation laisse encore quelques doutes, l'étape suivante consistera à apprécier si des garanties supplémentaires, apportant davantage de protection à la

[69] Compte tenu de leur importance, certaines questions spécifiques liées aux garanties seront examinées plus en détail dans des rubriques distinctes des sections III.3.5 et III.3.6.

personne concernée, peuvent faire pencher la balance dans un sens qui légitimerait le traitement.

a) Appréciation de l'intérêt légitime du responsable du traitement

Alors que la notion d'intérêt légitime est plutôt large, comme expliqué à la section III.3.1 ci-dessus, sa nature joue un rôle crucial quand il s'agit de mettre en balance ce type d'intérêt avec les droits et intérêts des personnes concernées. S'il est impossible de porter des jugements de valeur à l'égard de toutes les formes d'intérêt légitime envisageables, il est possible de formuler certaines orientations. Comme indiqué précédemment, cet intérêt peut être insignifiant ou impérieux, manifeste ou plus controversé.

i) Exercice d'un droit fondamental

Plusieurs droits et libertés fondamentaux parmi ceux consacrés par la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)[70] et par la Convention européenne des droits de l'homme (ci-après la «CEDH») peuvent entrer en conflit avec le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, comme la liberté d'expression et d'information[71], la liberté des arts et des sciences[72], le droit d'accès aux documents[73], ainsi, par exemple, que le droit à la liberté et à la sûreté[74], la liberté de pensée, de conscience et de religion[75], la liberté d'entreprise[76], le droit de propriété[77], le droit à un recours effectif et à accéder à un tribunal impartial[78], ou la présomption d'innocence et les droits de la défense[79].

Pour que l'intérêt légitime du responsable du traitement prévale, le traitement des données doit être «nécessaire» et «proportionné» à l'exercice du droit fondamental concerné.

À titre d'illustration, selon les circonstances, il peut s'avérer nécessaire et proportionné qu'un journal publie certains éléments incriminants à propos du train de vie d'un haut fonctionnaire impliqué dans un scandale de corruption présumé. D'un autre côté, il ne s'agit pas de donner aux médias toute latitude de publier sans motif valable n'importe quel détail sur la vie privée des personnalités publiques. Ce genre de cas suscite généralement des questions d'appréciation complexes et il peut être utile, pour éclairer l'évaluation, de s'appuyer sur une législation et une jurisprudence spécifiques, sur des lignes directrices, des codes de conduite et d'autres critères formels ou informels[80].

---

[70] Les dispositions de la Charte s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union.
[71] Article 11 de la Charte et article 10 de la CEDH.
[72] Article 13 de la Charte et articles 9 et 10 de la CEDH.
[73] Article 42 de la Charte: «Tout citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a un droit d'accès aux documents des institutions, organes et organismes de l'Union, quel que soit leur support..» Des droits d'accès similaires existent dans plusieurs États membres concernant les documents détenus par les organes publics de ces États membres.
[74] Article 6 de la Charte et article 5 de la CEDH.
[75] Article 10 de la Charte et article 9 de la CEDH.
[76] Article 16 de la Charte.
[77] Article 17 de la Charte et article 1er du protocole n°1 à la CEDH.
[78] Article 47 de la Charte et article 6 de la CEDH.
[79] Article 48 de la Charte et articles 6 et 13 de la CEDH.
[80] À propos des critères à appliquer dans les situations touchant à la liberté d'expression, la jurisprudence de la Cour européenne des droits de l'homme apporte aussi des orientations utiles. Voir, par exemple, l'arrêt de la

Dans ce contexte aussi, des garanties supplémentaires peuvent, éventuellement, jouer un rôle important et aider à trouver des moyens de parvenir à un équilibre – parfois fragile.

ii) Intérêt public/intérêt de la collectivité

Dans certains cas, le responsable du traitement peut choisir d'invoquer l'intérêt public ou l'intérêt de la collectivité (que ce soit prévu ou non par les lois ou les réglementations nationales). Par exemple, des données à caractère personnel peuvent être traitées par une association caritative aux fins de la recherche médicale, ou par une organisation sans but lucratif dans le cadre d'une action de mobilisation contre la corruption.

Il peut aussi arriver que l'intérêt commercial d'une société privée coïncide dans une certaine mesure avec un intérêt public. Cela peut être le cas, par exemple, pour lutter contre la fraude financière ou l'utilisation abusive de services[81]. Un prestataire de services peut avoir un intérêt commercial légitime à veiller à ce que ses clients n'abusent pas du service (ou ne puissent pas obtenir des services sans payer), mais, en même temps, les clients de l'entreprise, les contribuables et l'ensemble des citoyens ont aussi un intérêt légitime à ce que les activités frauduleuses soient découragées et détectées quand elles sont commises.

En général, le fait qu'un responsable du traitement agisse non seulement dans son propre intérêt légitime (commercial, par exemple), mais aussi dans l'intérêt de la collectivité, peut donner plus de «poids» à cet intérêt. Plus l'intérêt public ou collectif est impérieux, et plus la collectivité et les personnes concernées reconnaissent sans équivoque au responsable du traitement la possibilité d'agir et de procéder au traitement de données pour servir ces intérêts et s'attendent à ce qu'il l'utilise, plus l'intérêt légitime pèse dans la balance.

D'un autre côté, «l'application du droit par la sphère privée» ne doit pas servir à légitimer des pratiques qui, si elles étaient le fait d'un organisme public, seraient interdites au regard de la jurisprudence de la Cour européenne des droits de l'homme, au motif qu'elles constitueraient une ingérence d'une autorité publique dans la vie privée des personnes concernées sans satisfaire au critère rigoureux prévu par l'article 8, paragraphe 2, de la CEDH.

iii) Autres intérêts légitimes

Dans certains cas, ainsi qu'il a été expliqué à la section III.2, le contexte dans lequel un intérêt légitime apparaît peut se rapprocher de ceux où certains autres fondements juridiques peuvent être retenus, en particulier les motifs visés aux points b) (contrat), c) (obligation légale), ou e) (mission d'intérêt public), de l'article 7. Par exemple, il se peut qu'une activité de traitement des données ne soit pas strictement nécessaire, mais qu'elle reste néanmoins pertinente pour l'exécution d'un contrat, comme il est possible qu'une loi autorise, le traitement de certaines

---

Cour dans l'affaire von Hannover/Allemagne (n° 2) du 7 février 2012, notamment les points 95 à 126. Il faut aussi tenir compte du fait que l'article 9 de la directive (sous l'intitulé *Traitement de données à caractère personnel et liberté d'expression*) autorise les États membres à «prévoi[r], pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations [à certaines dispositions de la directive]» pour autant qu'elles soient «nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression».

[81] Voir, par exemple, «Exemple 21: extraction des données de compteurs intelligents pour détecter l'utilisation frauduleuse d'énergie» en page 67 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note 9).

données,sans pour autant l'exiger. Comme on l'a vu, il n'est pas toujours facile de tracer une ligne de séparation claire entre les différents motifs, mais il n'en est que plus important d'inclure dans l'analyse le test de mise en balance visé à l'article 7, point f).

Ici encore, comme dans tous les autres cas possibles qui n'ont pas été mentionnés jusqu'à présent, plus l'intérêt poursuivi par le responsable du traitement est impérieux, et plus la collectivité reconnaît sans équivoque au responsable du traitement la possibilité d'agir et de et procéder au traitement des données pour servir cet intérêt légitime et s'attend à ce qu'il l'utilise, plus ledit intérêt pèse dans la balance[82]. Cela nous amène au point suivant, d'ordre plus général.

iv) Reconnaissance juridique et culturelle/sociétale de la légitimité des intérêts

Dans tous les contextes présentés ci-dessus, il importe également de savoir si le droit de l'Union ou d'un État membre permet expressément (même s'il ne l'exige pas) que les responsables du traitement prennent des mesures pour poursuivre l'intérêt public ou privé concerné. L'existence d'orientations non contraignantes dûment adoptées, élaborées par des autorités telles que des agences disposant de pouvoirs réglementaires, qui encouragent les responsables du traitement à traiter les données pour poursuivre l'intérêt concerné entre aussi en ligne de compte.

Le respect d'éventuelles orientations non contraignantes formulées par des autorités chargées de la protection des données ou d'autres organismes compétents concernant les modalités du traitement des données pourra probablement contribuer à une appréciation favorable lors de la mise en balance. Les attentes culturelles et sociétales, même si elles ne se reflètent pas directement dans les instruments législatifs ou réglementaires, peuvent aussi jouer un rôle et faire pencher la balance dans un sens ou dans l'autre.

Plus il est reconnu explicitement dans la législation ou dans d'autres instruments réglementaires – contraignants ou non pour les responsables du traitement – ou même dans la culture de la collectivité concernée, sans qu'il existe de base juridique précise, que les responsables du traitement peuvent prendre des mesures et traiter des données afin de poursuivre un intérêt particulier, plus cet intérêt légitime pèse lourd dans la balance[83].

b) Incidence sur les personnes concernées

L'autre plateau de la balance, à savoir l'incidence du traitement sur l'intérêt ou les droits et libertés fondamentaux de la personne concernée, constitue un critère crucial. La première sous-section présentée ci-dessous aborde en termes généraux les modalités d'évaluation de l'impact sur la personne concernée.

Plusieurs éléments peuvent être utiles ici. Ils seront analysés dans d'autres sous-sections, notamment la nature des données à caractère personnel, la façon dont les informations sont traitées, les attentes raisonnables des personnes concernées et le statut du responsable du traitement et de la personne concernée. Nous examinerons aussi brièvement certaines

[82] Bien sûr, l'appréciation doit aussi comprendre une réflexion sur le préjudice que le responsable du traitement, des tiers ou la collectivité pourraient subir si le traitement des données n'est pas effectué.

[83] Cet intérêt ne peut cependant pas servir à légitimer des pratiques d'ingérence qui, autrement, ne satisferaient pas au critère de l'article 8, paragraphe 2, de la CEDH.

questions liées aux sources de risques potentiels qui peuvent avoir des conséquences pour les individus concernés, à la gravité de ces conséquences potentielles et à la probabilité de les voir se concrétiser.

i) Évaluation de l'incidence

Pour apprécier l'incidence[84] du traitement, il convient de prendre en considération les conséquences aussi bien positives que négatives. Il peut s'agir notamment de décisions ou de mesures éventuelles qui seront prises ultérieurement par des tiers et de situations où le traitement peut aboutir à l'exclusion de certaines personnes, à une discrimination à leur encontre, à de la diffamation ou, plus généralement, de situations qui comportent un risque de nuire à la réputation, au pouvoir de négociation ou à l'autonomie de la personne concernée.

En plus des conséquences négatives qui peuvent être spécifiquement prévues, il faut aussi tenir compte des répercussions morales, comme l'irritation, la crainte et le désarroi qui peuvent résulter de la perte du contrôle exercé par la personne concernée sur ses informations à caractère personnel, ou de la découverte d'une utilisation abusive ou d'une compromission effective ou potentielle de ces informations – du fait, par exemple, de leur divulgation sur l'internet. L'effet dissuasif sur un comportement protégé, comme la liberté de recherche ou la liberté d'expression, qui peut résulter d'une surveillance constante ou d'un traçage, doit aussi être dûment pris en considération.

Le groupe de travail insiste sur l'importance cruciale de comprendre que l'«incidence» dont il faut tenir compte constitue une notion beaucoup plus large qu'un préjudice ou un dommage occasionné à une ou plusieurs personnes concernées en particulier. Le terme «incidence», tel qu'il est employé dans le présent avis, couvre toutes les conséquences possibles (potentielles ou effectives) du traitement de données. Dans un souci de clarté, nous soulignons aussi le fait que cette notion n'est pas liée à celle de violation de données et va au-delà des incidences qui peuvent résulter d'une violation de données. La notion d'incidence, telle qu'elle est utilisée ici, englobe plutôt les diverses façons dont un individu peut être affecté – positivement ou négativement – par le traitement de ses données à caractère personnel[85].

Il importe aussi de comprendre que, bien souvent, l'incidence négative subie par la personne concernée résulte de l'accumulation d'un ensemble de circonstances liées ou non et qu'il peut

[84] Cette évaluation de l'incidence doit s'entendre dans le contexte de l'article 7, point f). Autrement dit, nous ne nous référons pas à une «analyse des risques» ou à une «analyse d'impact relative à la protection des données» au sens de la proposition de règlement (articles 33 et 34) et des divers amendements proposés par la commission LIBE. La question de la méthodologie à suivre dans le cadre d'une «analyse des risques» ou d'une «analyse d'impact relative à la protection des données» déborde du cadre du présent avis. D'un autre côté, il ne faut pas perdre de vue que – d'une manière ou d'une autre –, l'analyse d'impact au regard de l'article 7, point f), peut constituer une part importante d'une «analyse des risques» ou d'une «analyse d'impact relative à la protection des données» éventuelle et peut aussi contribuer à identifier des situations où il y a lieu de consulter l'autorité chargée de la protection des données.

[85] Par exemple, le risque de préjudice financier si une violation de données provoque la diffusion d'informations financières censées être conservées dans un environnement sûr, et aboutit à un vol d'identité ou à d'autres formes de fraude, ou les risques de lésion, de douleur, de souffrance et d'inconfort qui pourraient découler, par exemple, d'une altération non autorisée de dossiers médicaux entraînant une erreur dans le traitement d'un patient, doivent toujours être dûment pris en compte, bien que cela ne se limite en aucune façon à des situations entrant dans le champ d'application de l'article 7, point f). Ces risques ne sont cependant pas les seuls à prendre en considération pour l'évaluation d'impact au regard de l'article 7, point f).

se révéler difficile d'établir quelle activité de traitement a été déterminante pour cette incidence négative et par quel responsable du traitement elle a été effectuée.

Étant donné que, dans ce contexte, il est souvent difficile, pour les personnes concernées, de constituer un dossier de demande d'indemnisation pour un préjudice ou un dommage subi, même si l'effet lui-même est très réel, il n'en est que plus important de privilégier la prévention et de veiller à ce que les activités de traitement des données ne puissent avoir lieu que si le risque d'une incidence négative indue sur l'intérêt ou les droits et libertés fondamentaux des personnes concernées est nul ou très faible.

Pour évaluer l'incidence, la terminologie et la méthodologie employées en matière d'analyse des risques traditionnelle peuvent être utiles dans une certaine mesure. C'est pourquoi quelques éléments de cette méthodologie seront évoqués succinctement ci-après. L'élaboration d'une méthodologie complète d'évaluation d'impact – dans le contexte de l'article 7, point f), ou d'une manière plus générale – sortirait cependant du cadre du présent avis.

Dans ce contexte comme dans d'autres, il est important d'identifier les sources d'incidences potentielles sur les personnes concernées.

La probabilité qu'un risque se concrétise est un des éléments à prendre en considération. Par exemple, l'accessibilité via l'internet, les échanges de données avec des sites hébergés en dehors de l'Union, les interconnexions avec d'autres systèmes et un degré élevé d'hétérogénéité ou de variabilité peuvent représenter des vulnérabilités que des pirates pourraient exploiter. À cette source de risque correspond une probabilité élevée de voir le risque de compromission de données se matérialiser. À l'inverse, un système homogène et stable qui n'a pas d'interconnexions et est déconnecté de l'internet comporte un risque beaucoup plus faible de compromission de données.

Un autre élément de l'analyse des risques tient à la gravité des conséquences d'un risque qui se concrétise. Il peut s'agir, dans les cas les moins préoccupants, de la simple contrariété liée à la nécessité de réencoder les coordonnées perdues par le responsable du traitement des données mais, dans les cas les plus extrêmes, les conséquences peuvent être fatales, par exemple quand la localisation d'individus placés sous protection tombe entre les mains de criminels ou en cas de coupure de l'alimentation électrique à distance via des compteurs intelligents alors que les conditions météorologiques ou l'état de santé des personnes concernées sont critiques.

Chacun de ces deux éléments-clés – la probabilité que le risque se concrétise d'une part, et la gravité des conséquences de l'autre – contribue à l'évaluation générale de l'incidence potentielle.

Enfin, en appliquant la méthodologie, il ne faut pas perdre de vue que l'évaluation d'impact au regard de l'article 7, point f), ne saurait aboutir à un exercice mécanique et purement quantitatif. Dans les scénarios d'analyse des risques traditionnels, la «gravité» peut prendre en compte le nombre d'individus susceptibles d'être affectés. Néanmoins, il convient de rappeler qu'un traitement des données à caractère personnel ayant une incidence sur un petit nombre de personnes – voire sur un seul individu – requiert quand même une analyse très minutieuse, surtout si l'incidence sur chaque individu concerné est potentiellement importante.

ii) Nature des données

Il serait important, tout d'abord, d'évaluer si le traitement porte sur des données sensibles, soit qu'elles relèvent des catégories particulières de données visées à l'article 8 de la directive, soit pour d'autres raisons, comme dans le cas des données biométriques, des informations génétiques, des données de communication, des données de localisation et d'autres formes d'informations personnelles nécessitant une protection spéciale[86].

À titre d'illustration, le groupe de travail considère, en règle générale, que l'utilisation de la biométrie pour satisfaire à des exigences générales en matière de sécurité des biens ou des personnes constitue un intérêt légitime sur lequel prévaudrait l'intérêt ou les droits et libertés fondamentaux de la personne concernée. D'un autre côté, des données biométriques comme les empreintes digitales et/ou l'image de l'iris pourraient servir à assurer la sécurité d'un lieu à haut risque comme un laboratoire effectuant des recherches sur des virus dangereux, pour autant que le responsable du traitement ait apporté la preuve concrète de l'existence d'un risque considérable[87].

En général, plus les informations sont sensibles, plus les conséquences qu'elles peuvent avoir pour la personne concernée sont importantes. Cela ne veut pas dire, cependant, qu'il est permis de traiter librement, en vertu de l'article 7, point f), des données qui, en elles-mêmes, peuvent paraître anodines. En effet, selon la façon dont elles sont traitées, même ces données peuvent avoir une incidence importante sur les individus, comme on le verra dans la sous-section iii) ci-dessous.

À cet égard, le fait que les données aient déjà été rendues publiques par la personne concernée ou par des tiers peut être un élément pertinent. Il importe avant tout de souligner ici que les données à caractère personnel, même si elles ont été rendues publiques, restent considérées comme des données à caractère personnel et que leur traitement continue donc à requérir des garanties appropriées[88]. Il n'existe aucune autorisation générale permettant de réutiliser et de traiter de nouveau des données à caractère personnel publiquement disponibles en vertu de l'article 7, point f).

Cela dit, le fait que des données à caractère personnel soient publiquement disponibles est un facteur qui peut être pris en considération dans l'évaluation, surtout si leur publication s'accompagnait d'une attente raisonnable d'utilisation ultérieure des données à certaines fins

[86] Les données biométriques et les informations génétiques sont considérées comme des catégories particulières de données dans la proposition de règlement sur la protection des données de la Commission, lue conjointement avec les amendements proposés par la commission LIBE. Voir l'amendement 103 sur l'article 9 dans le rapport final de la commission LIBE. À propos de la relation entre les articles 7 et 8 de la directive 95/46/CE, voir la section III.1.2 ci-dessus, en pages 15 à 17.

[87] Voir l'avis 3/2012 du groupe de travail «Article 29» sur l'évolution des technologies biométriques (WP 193). Pour donner un autre exemple, dans son avis 4/2009 sur l'Agence mondiale antidopage (cité précédemment en note de bas de page 32), le groupe de travail a souligné que l'article 7, point f), ne constituerait pas un motif valable pour justifier le traitement des données médicales et des données relatives aux infractions dans le contexte des enquêtes antidopage, au regard de la «gravité des intrusions dans la vie privée» qui en résulteraient. Le traitement des données doit être prévu par la loi et doit satisfaire aux exigences de l'article 8, paragraphe 4 ou 5, de la directive.

[88] Voir l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus) et l'avis 06/2013 du groupe de travail «Article 29» sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, adopté le 5.6.2013 (WP 207).

(par exemple, pour des travaux de recherche ou dans un souci de transparence et de responsabilité).

iii) La façon dont les données sont traitées

L'analyse d'impact au sens large peut consister notamment à examiner si les données ont été publiées ou rendues accessibles par quelque autre moyen à un grand nombre de personnes, ou si des volumes considérables de données à caractère personnel sont traités ou combinés avec d'autres données (par exemple, en cas d'établissement de profils, à des fins commerciales, judiciaires, ou autres). Le traitement à grande échelle de données apparemment anodines et leur combinaison avec d'autres données peuvent parfois permettre des inférences à propos de données plus sensibles, comme l'a montré le scénario 3 ci-dessus, qui illustrait la mise en relation des habitudes de consommation de pizzas avec les primes d'assurance santé.

Outre le fait qu'elle risque de permettre le traitement de données plus sensibles, ce genre d'analyse peut aussi conduire à des prévisions saugrenues, inattendues, voire inexactes concernant, par exemple, le comportement ou la personnalité des individus concernés. Selon la nature et l'incidence de ces prévisions, l'intrusion dans la vie privée de ces personnes peut être considérable[89].

Le groupe de travail a aussi insisté, dans un avis précédent, sur les risques inhérents à certaines solutions de sécurité (notamment les pare-feu, antivirus ou anti-spam), susceptibles de donner lieu au déploiement à grande échelle de l'analyse des paquets en profondeur , ce qui peut influencer sensiblement l'appréciation de l'équilibre des droits[90].

En général, plus l'incidence du traitement pourrait se révéler négative ou incertaine, moins il est probable que ce traitement sera jugé légitime au regard du critère de mise en balance. Dans ce contexte, il sera certainement utile d'examiner s'il n'existe pas d'autres méthodes, aux conséquences moins négatives pour la personne concernée, pour atteindre les objectifs poursuivis par le responsable du traitement. Si nécessaire, des analyses d'impact relatives à la vie privée et à la protection des données peuvent servir à déterminer si cette possibilité peut être envisagée.

iv) Attentes raisonnables de la personne concernée

Les attentes raisonnables de la personne concernée quant à l'utilisation et à la divulgation des données sont aussi très pertinentes à cet égard. Ainsi qu'il a été indiqué à propos de l'analyse du principe de limitation de la finalité[91], il est «important d'examiner si le statut du responsable du traitement des données[92], la nature de la relation ou du service fourni[93] ou les

[89] Voir la section III.2.5 et l'annexe 2 (gros volumes de données et données ouvertes) de l'avis sur la limitation de la finalité (cité précédemment en note de bas de page 9).
[90] Voir la section 3.1 de l'avis 1/2009 du groupe de travail «Article 29» concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (WP 159).
[91] Voir les pages 24 et 25 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).
[92] «Comme, par exemple, un avocat ou un médecin».
[93] «Comme, par exemple, des services d'informatique en nuage pour la gestion des documents personnels, des services de messagerie électronique, des agendas électroniques, des liseuses équipées de fonctions de prise de notes et diverses applications de journal qui peuvent contenir des informations très personnelles.»

obligations légales ou contractuelles applicables (ou d'autres engagements pris lors de la collecte) pourraient susciter des attentes raisonnables de confidentialité plus stricte et de limitations plus strictes en cas d'utilisation ultérieure». En général, plus le contexte de la collecte est spécifique et restrictif, plus les limitations susceptibles de s'appliquer à l'utilisation des données sont strictes. Là encore, il est nécessaire de tenir compte des circonstances factuelles, plutôt que de s'appuyer simplement sur des clauses imprimées en petits caractères.

v) Statut du responsable du traitement des données et de la personne concernée

Le statut de la personne concernée et du responsable du traitement des données est aussi pertinent pour apprécier l'incidence du traitement. Selon que le responsable du traitement des données est un individu ou une petite organisation, une grande multinationale, ou un organisme du secteur public et en fonction des circonstances, le rapport de force avec la personne concernée peut être plus ou moins grand. Une grande multinationale dispose, par exemple, de ressources et d'un pouvoir de négociation considérables vis-à-vis d'une personne concernée, à titre individuel, et elle peut par conséquent être à même d'imposer ce qu'elle considère comme son «intérêt légitime» à la personne concernée, surtout si l'entreprise occupe une position dominante sur le marché. En l'absence de contrôle, ce genre de situation peut tourner au désavantage des personnes concernées. De même que les lois sur la protection des consommateurs et sur la concurrence contribuent à éviter que ce pouvoir ne soit pas utilisé à bon escient, le droit applicable en matière de protection des données pourrait aussi jouer un rôle important en matière de prévention des atteintes aux droits et aux intérêts des personnes concernées.

D'un autre côté, le statut de la personne concernée a aussi son importance. Si, en principe, il y a lieu d'appliquer le critère de mise en balance par rapport à un individu moyen, certaines situations spécifiques appellent plutôt une approche au cas par cas: par exemple, il serait pertinent de prendre en considération le fait que la personne concernée est un enfant[94] ou appartient à une catégorie de population plus vulnérable qui requiert une protection spéciale, comme, par exemple, les malades mentaux, les demandeurs d'asile ou les personnes âgées. Bien sûr, il faut aussi examiner si la personne concernée est un salarié, un étudiant, un patient ou s'il existe de quelque autre façon un déséquilibre dans la relation entre la position de la personne concernée et celle du responsable du traitement. Il est important d'apprécier l'effet concret du traitement sur les individus en particulier.

Enfin, il faut souligner que toutes les incidences négatives sur les personnes concernées ne «pèsent» pas du même poids dans la balance. La finalité du critère de mise en balance prévu par l'article 7, point f), n'est pas d'éviter toute incidence négative sur la personne concernée. Il s'agit plutôt de prévenir une incidence disproportionnée. La différence est cruciale. Par exemple, la publication dans un journal d'un article fondé sur une enquête sérieuse et sur des faits précis à propos de soupçons de corruption au sein de l'administration peut être préjudiciable à la réputation des fonctionnaires concernés et peut avoir des conséquences

[94] Voir l'avis 2/2009 du groupe de travail «Article 29» sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), adopté le 11.2.2009 (WP 160). Cet avis insiste sur la vulnérabilité spécifique de l'enfant et, dans le cas où l'enfant est représenté, sur la nécessité de prendre en compte son intérêt propre et non celui de ses représentants.

importantes, notamment l'atteinte à la réputation, la défaite aux élections, ou l'emprisonnement, mais elle pourrait néanmoins être fondée en vertu de l'article 7, point f)[95].

c) Bilan provisoire

Lors de la mise en balance des intérêts et des droits en jeu, comme décrit précédemment, les mesures prises par le responsable du traitement pour se conformer aux obligations générales que lui impose la directive, notamment en termes de proportionnalité et de transparence, contribueront grandement à garantir le respect par le responsable du traitement des données des exigences énoncées à l'article 7, point f). Un respect absolu de ces conditions devrait signifier que l'incidence sur les individus est réduite, qu'une ingérence dans la poursuite des intérêts et l'exercice des droits ou libertés fondamentaux des personnes concernées est *moins probable* et qu'il est, par conséquent, *plus probable* que l'article 7, point f), puisse être invoqué par le responsable du traitement des données. Cela devrait encourager les responsables du traitement à mieux se conformer à toutes les dispositions horizontales de la directive[96].

Cela ne veut pas dire, cependant, que le respect de ces exigences horizontales sera toujours, en soi, suffisant pour garantir une base juridique en application de l'article 7, point f). Si tel était le cas, en effet, l'article 7, point f), serait superflu ou créerait une faille privant de sa signification l'article 7 tout entier, qui prévoit que le traitement doit se fonder sur une base juridique précise adéquate.

C'est pourquoi il importe d'approfondir l'évaluation lors de l'exercice de mise en balance lorsque l'analyse préliminaire ne permet pas d'établir clairement dans quel sens penche la balance. Le responsable du traitement peut envisager d'introduire des mesures supplémentaires, qui vont au-delà du respect des dispositions horizontales de la directive, afin de contribuer à réduire toute incidence indue du traitement sur les personnes concernées.

Ces mesures supplémentaires peuvent comprendre, par exemple, la mise à disposition d'un mécanisme accessible et facile à utiliser offrant aux personnes concernées la possibilité inconditionnelle de s'opposer au traitement. Dans certains cas (mais pas toujours), de telles mesures peuvent contribuer à faire pencher la balance et à permettre le traitement en vertu de l'article 7, point f), tout en protégeant aussi les droits et les intérêts des personnes concernées.

d) Garanties supplémentaires mises en place par le responsable du traitement

Comme expliqué ci-dessus, la façon dont le responsable du traitement appliquerait des mesures appropriées pourrait, dans certaines situations, contribuer à «faire pencher la balance». C'est l'évaluation dans son ensemble qui déterminera si le résultat est acceptable ou non. Plus l'incidence sur la personne concernée est significative, plus il convient de prêter attention aux garanties pertinentes.

[95] Comme expliqué précédemment, les éventuelles dérogations pertinentes pour le traitement à des fins de journalisme en vertu de l'article 9 de la directive doivent aussi être prises en compte.

[96] À propos du rôle important du «respect des dispositions horizontales», voir aussi la page 54 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité, cité en note de bas de page 9, ci-dessus.

À titre d'exemple, les mesures concernées peuvent inclure, entre autres, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation. Si certaines de ces mesures sont peut-être déjà obligatoires au titre de la directive, elles sont souvent modulables et laissent aux responsables du traitement une certaine latitude pour assurer une meilleure protection des personnes concernées. Par exemple, le responsable du traitement peut collecter moins de données, ou fournir des informations complémentaires par rapport à ce que prévoient spécifiquement les articles 10 et 11 de la directive.

Dans certains autres cas, les garanties ne sont pas *explicitement* requises par la directive, mais pourraient bien figurer à l'avenir dans le règlement proposé, ou elles ne sont exigées que dans des situations particulières. Il peut s'agir, par exemple:

- de mesures techniques et organisationnelles garantissant que les données ne peuvent servir à la prise de décisions ou de mesures à l'endroit des individus («séparation fonctionnelle», comme c'est souvent le cas dans le contexte de la recherche);
- d'un large recours aux techniques d'anonymisation;
- de l'agrégation de données;
- de technologies renforçant la protection de la vie privée, de la prise en compte du respect de la vie privée dès la conception, d'analyses d'impact relatives à la vie privée et à la protection des données;
- d'une transparence accrue;
- d'un droit d'opposition général et inconditionnel;
- de la portabilité des données et d'autres mesures connexes destinées à renforcer le pouvoir des personnes concernées.

Le groupe de travail observe qu'en ce qui concerne certaines questions-clés, notamment la séparation fonctionnelle et les techniques d'anonymisation, certaines orientations ont déjà été données dans les parties correspondantes de ses avis sur la limitation de la finalité, sur les données ouvertes et sur les techniques d'anonymisation[97].

En ce qui concerne la pseudonymisation et le chiffrement, le groupe de travail tient à souligner que, si les données ne sont pas directement identifiables, cela n'a, en soi, aucune incidence sur l'appréciation de la légitimité du traitement: il ne faudrait pas croire que ces techniques permettent de rendre légitime un traitement qui ne l'est pas[98].

Cependant, la pseudonymisation et le chiffrement, comme toutes les autres mesures techniques et organisationnelles introduites pour protéger les informations personnelles, joueront un rôle dans l'évaluation de l'incidence potentielle du traitement sur la personne concernée et, de ce fait, pourront dans certains cas contribuer à faire pencher la balance en faveur du responsable du traitement. L'utilisation de formes moins risquées de traitement des données à caractère personnel (par exemple, le chiffrement des données à caractère personnel

[97] Voir les sections III.2.3, III.2.5 et l'annexe 2 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité, cité précédemment en note de bas de page 9, à propos du traitement ultérieur à des fins de recherche historique, statistique et scientifique, des gros volumes de données et des données ouvertes; voir aussi les sections concernées de l'avis 06/2013 du groupe de travail «Article 29» sur les données ouvertes (cité en note de bas de page 88 ci-dessus) et de l'avis 5/2014 sur les techniques d'anonymisation.

[98] Voir sur ce point les amendements votés par la commission LIBE dans le rapport final de la commission LIBE, et en particulier l'amendement 15 sur le considérant 38, qui met en relation la pseudonymisation et les attentes légitimes de la personne concernée.

en vue de leur stockage ou de leur transit, ou le fait de rendre les données à caractère personnel moins directement et moins aisément identifiables) devrait généralement réduire les risques d'interférence avec l'intérêt ou les droits et libertés fondamentaux des personnes concernées.

À propos de ces garanties – et de l'appréciation générale résultant de la mise en balance – le groupe de travail souhaite mettre en avant trois aspects spécifiques qui jouent souvent un rôle crucial dans le contexte de l'article 7, point f):

- la relation entre le critère de mise en balance, la transparence et le principe de responsabilité;
- le droit de la personne concernée de s'opposer au traitement, et au-delà de cette opposition, la possibilité de refuser sans avoir à donner de justification; et
- le renforcement du pouvoir des personnes concernées: portabilité des données et disponibilité de mécanismes fonctionnels permettant à la personne concernée d'accéder à ses propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur).

Compte tenu de leur importance, ces sujets seront examinés dans des sections séparées.

III.3.5. Responsabilité et transparence

Tout d'abord, avant qu'une opération de traitement en vertu de l'article 7, point f), puisse avoir lieu, il appartient au responsable du traitement d'apprécier s'il a un intérêt légitime, si le traitement est nécessaire à cet intérêt légitime et si, dans le cas envisagé, les intérêts et les droits des personnes concernées ne prévalent pas sur cet intérêt.

C'est pourquoi l'article 7, point f), repose sur le principe de responsabilité. Le responsable du traitement doit au préalable procéder à une analyse minutieuse et effective, fondée sur les circonstances factuelles particulières plutôt que sur une réflexion abstraite, en tenant compte aussi des attentes raisonnables des personnes concernées. Une bonne pratique consisterait, éventuellement, à documenter ce travail d'analyse d'une manière suffisamment détaillée et transparente pour permettre la vérification de l'application complète et correcte du critère de mise en balance par les parties intéressées, notamment les personnes concernées et les autorités chargées de la protection des données, et enfin par les tribunaux, si besoin est.

Le responsable du traitement définira d'abord l'intérêt légitime qu'il poursuit et appliquera ensuite le critère de mise en balance, mais il ne s'agit pas là nécessairement d'une appréciation définitive: si, en réalité, l'intérêt poursuivi n'est pas celui qui a été spécifié par le responsable du traitement ou si la définition de l'intérêt n'est pas suffisamment détaillée, il faut réévaluer la mise en balance, sur la base de l'intérêt réel, qui sera déterminé soit par une autorité chargée de la protection des données soit par un tribunal[99]. Comme dans le cas d'autres aspects essentiels de la protection des données, par exemple l'identification du responsable du traitement des données ou la spécification de la finalité[100], ce qui importe, c'est la réalité que recouvre toute affirmation faite par le responsable du traitement.

[99] Par exemple, à la suite d'une plainte ou d'une opposition exprimée en vertu de l'article 14.
[100] Voir les avis cités en note de bas de page 9.

La notion de responsabilité est étroitement liée à celle de transparence. Afin de permettre aux personnes concernées de faire valoir leurs droits et, plus généralement, aux parties prenantes d'exercer un contrôle public, le groupe de travail recommande que les responsables du traitement expliquent aux personnes concernées d'une manière claire et conviviale les raisons qu'ils ont de penser que l'intérêt ou les droits et libertés fondamentaux des personnes concernées ne prévalent pas sur l'intérêt qu'ils poursuivent et leur présentent aussi les garanties qu'ils ont prises pour protéger les données à caractère personnel, y compris, le cas échéant, le droit de s'opposer au traitement[101].

À cet égard, le groupe de travail souligne que la législation en matière de protection des consommateurs et, en particulier, les lois qui protègent les consommateurs contre les pratiques commerciales déloyales revêtent aussi une grande importance ici.

Si un responsable du traitement dissimule, dans une clause contractuelle formulée en termes juridiques techniques et imprimée en petits caractères, des informations importantes concernant une utilisation ultérieure inattendue des données, cette pratique peut tomber sous le coup des règles de protection des consommateurs relatives aux clauses abusives (notamment l'interdiction des «clauses surprenantes») et, par ailleurs, elle ne satisfait ni aux conditions de l'article 7, point a), qui supposent un consentement valide et informé, ni aux exigences de l'article 7, point f), du point de vue des attentes raisonnables de la personne concernée et d'un équilibre globalement acceptable des intérêts. Cela soulèverait bien sûr aussi des questions quant à la conformité avec l'article 6, qui requiert un traitement loyal et licite des données à caractère personnel.

Par exemple, dans un certain nombre de cas, les utilisateurs de services en ligne «gratuits», comme les moteurs de recherche, les messageries électroniques, les médias sociaux, le stockage de fichiers ou d'autres applications en ligne ou mobile, ne sont pas pleinement conscients de la mesure dans laquelle leur activité est enregistrée et analysée afin d'engendrer de la valeur pour le prestataire de services et, de ce fait, ils ne se préoccupent pas des risques que cela comporte.

Afin de renforcer le pouvoir des personnes concernées dans ces situations, une condition préalable nécessaire – mais nullement suffisante en elle-même – consiste d'abord à préciser que les services ne sont pas gratuits et que ce sont les données à caractère personnel des consommateurs qui servent de moyen de paiement[102]. Les conditions et les garanties sous réserve desquelles les données peuvent être utilisées doivent aussi être clairement énoncées

[101] Comme expliqué en page 46 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9), en cas d'établissement de profil et d'automatisation du processus décisionnel, «afin de garantir la transparence, les personnes concernées/consommateurs devraient avoir accès à leurs "profils", ainsi qu'à la logique du processus de décision (algorithme) qui aboutit à l'élaboration du profil. Autrement dit: les organisations devraient divulguer leurs critères décisionnels. C'est une garantie cruciale, qui revêt encore plus d'importance dans le monde des gros volumes de données». Le fait qu'une organisation assure ou non cette transparence est un facteur très pertinent à prendre également en considération dans l'exercice de mise en balance.

[102] Concernant d'autres garanties possibles dans les situations de plus en plus courantes où les consommateurs paient au moyen de leurs données personnelles, voir la section III.3.6, et en particulier, les pages 53 et 54, sous les rubriques «Alternatives respectueuses de la protection des données aux services en ligne "gratuits"» et «Portabilité des données, "midata" et questions connexes».

dans chaque cas pour assurer la validité du consentement requis par l'article 7, point a), ou un équilibre favorable au regard de l'article 7, point f).

III.3.6. Le droit d'opposition et au-delà

a) Le droit d'opposition en vertu de l'article 14 de la directive

Les points e) et f) de l'article 7 ont ceci de particulier que, s'ils reposent principalement sur une appréciation objective des intérêts et des droits en jeu, ils font aussi intervenir l'autodétermination de la personne concernée en lui reconnaissant un droit d'opposition[103]: pour ces deux motifs, au moins, l'article 14, point a), de la directive prévoit que («sauf en cas de disposition contraire du droit national») la personne concernée peut «s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement». Il ajoute que si cette opposition est justifiée, le traitement des données doit cesser.

En principe, selon la législation actuelle, la personne concernée devra donc démontrer qu'il existe «des raisons prépondérantes et légitimes» d'arrêter de traiter ses données à caractère personnel [article 14, point a)], sauf dans le cas d'activités de prospection, où l'opposition n'a pas à être justifiée [article 14, point b)].

Il ne faut pas y voir une contradiction avec le critère de mise en balance visé à l'article 7, point f), qui est appliqué a priori: cette disposition vient plutôt compléter la mise en balance, en ce sens que, lorsque le traitement est autorisé à la suite d'une évaluation raisonnable et objective des différents droits et intérêts en jeu, la personne concernée dispose encore d'une possibilité *supplémentaire* de marquer son opposition, pour des motifs liés à sa situation particulière. Il faudra alors procéder à une nouvelle appréciation en tenant compte des arguments spécifiques avancés par la personne concernée. Cette nouvelle appréciation peut, en principe, faire encore l'objet d'une vérification par une autorité chargée de la protection des données ou par les tribunaux.

b) Au-delà de l'opposition: le rôle du refus comme garantie supplémentaire

Le groupe de travail souligne que, même si le droit reconnu par l'article 14, point a), est subordonné à la présentation d'une justification par la personne concernée, rien n'empêche le responsable du traitement de proposer une option de refus qui serait plus large, et qui n'exigerait aucune démonstration supplémentaire d'un intérêt légitime (prépondérant ou autre) de la part de la personne concernée. Ce droit inconditionnel ne devrait pas se fonder sur la situation spécifique des personnes concernées.

En effet, surtout dans les cas douteux où il est difficile de trouver un équilibre, un mécanisme bien conçu et fonctionnel permettant de refuser le traitement, sans donner nécessairement aux personnes concernées tous les éléments qui satisferaient à la condition de consentement valide

[103] Ce droit d'opposition ne doit pas être confondu avec le consentement prévu par l'article 7, point a), que le responsable du traitement des données doit obtenir pour pouvoir traiter les données.. Dans le contexte de l'article 7, point f), le responsable du traitement peut traiter les données sous réserve de certaines conditions et garanties, aussi longtemps que la personne concernée ne s'y est pas opposée. En ce sens, le droit d'opposition peut plutôt être considéré comme une forme particulière d'option de refus. Voir plus de détails dans l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement (cité en note de bas de page 2).

visée à l'article 7, point a), pourrait jouer un rôle important pour préserver les droits et les intérêts des personnes concernées.

Pour ce faire, il est nécessaire d'adopter une approche nuancée, qui distingue entre les cas où un consentement préalable, conforme à l'article 7, point a), est requis et les cas où un mécanisme fonctionnel permettant de refuser le traitement (combiné éventuellement avec d'autres mesures supplémentaires) peut contribuer à protéger les personnes concernées au regard de l'article 7, point f).

Plus le mécanisme de l'option de refus est largement applicable et facile à exercer, plus il contribuera à faire pencher la balance en faveur du traitement et à permettre l'invocation de l'article 7, point f), comme fondement juridique.

Illustration: l'évolution de l'approche de la prospection directe

Afin d'illustrer la distinction qu'il convient d'établir entre les cas où un consentement au titre de l'article 7, point a), est requis et les cas où une option de refus pourrait servir de garantie au regard de l'article 7, point f), il est utile de prendre l'exemple de la prospection directe, pour laquelle il existe déjà une disposition spécifique prévoyant la possibilité de refuser le traitement, à l'article 14, point b), de la directive. Pour tenir compte des nouvelles avancées technologiques, cette disposition a été complétée ultérieurement par des dispositions spécifiques de la directive «vie privée et communications électroniques»[104].

Conformément à l'article 13 de la directive «vie privée et communications électroniques», pour certains types – plus intrusifs – d'activités de prospection directe (comme la prospection par courrier électronique et les automates d'appel), le consentement est de rigueur. À titre d'exception, dans le cadre d'une relation client-fournisseur existante, où un responsable du traitement cherche à promouvoir ses propres produits ou services «similaires», il est suffisant de prévoir une possibilité de refus (inconditionnelle), sans justification à fournir.

Les technologies ont évolué, nécessitant des solutions similaires, relativement simples, qui obéissent à une logique analogue pour les nouvelles pratiques de prospection.

Premièrement, la façon dont le matériel de prospection est diffusé a évolué: au lieu de simples courriers électroniques arrivant dans les boîtes aux lettres, des publicités comportementales ciblées apparaissent aussi désormais sur les écrans de smartphones et d'ordinateurs. Dans un proche avenir, la publicité pourrait être intégrée dans des objets intelligents connectés à l'internet des objets.

Deuxièmement, les publicités deviennent toujours plus spécifiquement ciblées: au lieu de se fonder sur de simples profils de clients, elles tirent parti du traçage des activités des consommateurs qui sont de plus en plus souvent conservées en ligne et hors ligne et analysées au moyen de méthodes automatisées plus élaborées[105].

[104] À propos de l'article 13 de la directive «vie privée et communications électroniques», voir aussi la section III.2.4 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).

[105] Voir la section III.2.5 et l'annexe 2 (sur les gros volumes de données et les données ouvertes) de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).

Du fait de ces évolutions, l'objectif de l'exercice de mise en balance est désormais différent: la question ne concerne plus la liberté d'expression commerciale, mais principalement l'intérêt économique des entreprises à mieux connaître leurs clients grâce au traçage et à la surveillance de leurs activités en ligne et hors ligne, qui devraient être mis en balance avec les droits (fondamentaux) de ces personnes au respect de leur vie privé et à la protection de leurs données à caractère personnel et avec leur intérêt à ne pas faire l'objet d'une surveillance indue.

Ce changement de modèle d'entreprise dominant et la valorisation des données à caractère personnel en tant qu'actif pour les sociétés commerciales expliquent l'exigence récente d'un consentement dans ce contexte, conformément à l'article 5, paragraphe 3, et à l'article 13 de la directive «vie privée et communications électroniques».

Il y a donc des règles spécifiques différentes, selon la forme de prospection, notamment:

- le droit inconditionnel de s'opposer au traitement à des fins de prospection (conçu pour le contexte traditionnel des envois postaux, et pour la promotion de produits similaires) conformément à l'article 14, point b), de la directive; l'article 7, point f), pourrait être invoqué comme fondement juridique dans ce cas;
- le consentement exigé en vertu de l'article 13 de la directive «vie privée et communications électroniques» pour la prospection au moyen d'automates d'appel, de télécopieurs, de messages texte et de courriers électroniques (sous réserve des exceptions prévues)[106], et l'application de fait de l'article 7, point a), de la directive sur la protection des données.
- le consentement exigé en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» [et de l'article 7, point a), de la directive sur la protection des données] pour la publicité comportementale fondée sur des techniques de traçage comme le stockage d'informations au moyen de cookies dans l'équipement terminal des utilisateurs[107].

Si les fondements juridiques applicables sont clairs en ce qui concerne l'article 5, paragraphe 3, et l'article 13 de la directive «vie privée et communications électroniques», toutes les formes de prospection ne sont pas couvertes et il serait souhaitable de pouvoir disposer d'orientations quant aux situations qui requièrent un consentement au titre de l'article 7, point a), et aux situations dans lesquelles un équilibre est atteint au regard de l'article 7, point f), grâce notamment à la possibilité de refuser le traitement.

À cet égard, il est utile de rappeler l'avis du groupe de travail «Article 29» sur la limitation de la finalité, où il est expressément indiqué que «si une organisation souhaite spécifiquement analyser ou prédire les préférences personnelles, le comportement et les attitudes de clients individuels, qui serviront ensuite à guider des "mesures ou décisions" prises à l'égard de ces clients [...] un consentement préalable libre, spécifique, informé et indubitable devrait presque toujours être requis, faute de quoi l'utilisation ultérieure ne pourra pas être jugée compatible. Ce consentement devrait surtout être requis, par exemple, pour le traçage et le profilage à des fins de prospection directe, de publicité comportementale, de courtage en informations, de

[106] Voir aussi l'article 13, paragraphe 3, de la directive «vie privée et communications électroniques», qui laisse aux États membres le choix entre les options de consentement et de refus pour la prospection directe passant par d'autres moyens.

[107] Concernant l'application de cette disposition, voir l'avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne (WP 171).

publicités fondées sur la localisation ou d'étude de marché numérique fondée sur le traçage[108].»

Alternatives respectueuses de la protection des données aux services en ligne «gratuits»

Dans le cas où les consommateurs qui souscrivent à des services en ligne «gratuits» «paient» en fait ces services en autorisant l'utilisation de leurs données à caractère personnel, un moyen de contribuer à une évaluation favorable à l'issue de la mise en balance – ou à la conclusion que le consommateur a vraiment été libre de son choix et a donc donné un consentement valide au titre de l'article 7, point a) – consisterait, pour le responsable du traitement, à proposer aussi une autre version de ses services, où les «données à caractère personnel» ne serviraient pas à des fins de prospection.

Tant que ces autres services ne sont pas disponibles, il est plus difficile de prétendre qu'un consentement valide (donné librement) a été obtenu au titre de l'article 7, point a), du simple fait de l'utilisation des services gratuits, ou que la balance penche en faveur du responsable du traitement au regard de l'article 7, point f).

Les considérations présentées ci-dessus soulignent le rôle important que des garanties supplémentaires, et notamment un mécanisme fonctionnel permettant de refuser le traitement, peuvent jouer pour modifier le bilan provisoire. Parallèlement, elles donnent aussi à penser que dans certains cas, l'article 7, point f), ne peut pas être invoqué comme motif justifiant le traitement et que les responsables du traitement doivent obtenir un consentement valide au titre de l'article 7, point a) – ou satisfaire à quelque autre condition énoncée par la directive – pour que le traitement puisse avoir lieu.

Portabilité des données, «midata» et questions connexes

Parmi les garanties supplémentaires qui pourraient contribuer à faire pencher la balance, il convient de prêter une attention particulière à la portabilité des données et aux mesures connexes, qui peuvent se révéler de plus en plus pertinentes dans un environnement en ligne. Le groupe de travail «Article 29» rappelle son avis sur la limitation de la finalité, où il a souligné que «dans de nombreuses situations, des garanties comme le fait de permettre aux personnes concernées/consommateurs d'accéder directement à leurs données dans un format portable, convivial et lisible par machine peuvent contribuer à renforcer leur pouvoir et à rectifier le déséquilibre économique entre les grandes entreprises, d'un côté, et les personnes concernées/consommateurs, de l'autre. Cela permettrait aussi aux individus de "partager les richesses" créées par les gros volumes de données et inciterait les développeurs à proposer des fonctionnalités et des applications complémentaires à leurs utilisateurs[109]».

[108] Voir l'annexe II (sur les gros volumes de données et les données ouvertes) de l'avis (cité en note de bas de page 9, ci-dessus), page 45.

[109] «Voir des initiatives comme "midata" au Royaume-Uni, qui reposent sur le principe-clé selon lequel les données devraient être restituées aux consommateurs. Le programme "midata" est une initiative volontaire, qui devrait progressivement offrir aux consommateurs un accès renforcé à leurs données personnelles dans un format électronique portable. L'idée maîtresse est que les consommateurs devraient aussi tirer profit des gros volumes de données en accédant à leurs propres informations pour être en mesure de faire de meilleurs choix. Voir aussi les initiatives "Green button" qui permettent aux consommateurs d'accéder à des informations sur leur propre consommation énergétique.» Pour plus d'information sur des initiatives au Royaume-Uni et en France, voir http://www.midatalab.org.uk/ et http://mesinfos.fing.org/.

La disponibilité de mécanismes fonctionnels permettant aux personnes concernées d'accéder à leurs propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur) renforcera le pouvoir des personnes concernées et leur donnera la possibilité de tirer un meilleur parti des services numériques. En outre, cela peut favoriser un environnement de marché plus concurrentiel, en permettant aux clients de changer plus aisément de fournisseurs (par exemple, en matière de services bancaires en ligne ou de fournisseurs d'énergie sur un réseau électrique intelligent). Enfin, cela peut aussi contribuer au développement d'autres services à valeur ajoutée par des tiers qui pourront accéder aux données des consommateurs à la demande de ces derniers et avec leur consentement. Dans cette perspective, la portabilité des données est donc une bonne chose non seulement pour la protection des données, mais aussi pour la concurrence et la protection des consommateurs[110].

IV. Observations finales

Dans le présent avis, le groupe de travail a analysé les critères légitimant le traitement des données énoncés dans l'article 7 de la directive. Au-delà des orientations proposées pour l'interprétation et l'application pratiques de l'article 7, point f), dans le cadre juridique actuel, son objectif est de formuler des recommandations politiques destinées à aider les décideurs dans le choix des modifications qu'ils envisagent d'apporter au cadre juridique actuel en matière de protection des données. Avant de présenter ces recommandations, les principales conclusions concernant l'interprétation de l'article 7 sont résumées ci-après.

IV.1. Conclusions

Aperçu général de l'article 7

L'article 7 dispose que le traitement de données à caractère personnel ne peut être effectué que si au moins un des six motifs juridiques énumérés à cet article existe.

Le premier motif, exposé à l'article 7, point a), porte sur le consentement de la personne concernée comme fondement légitimant le traitement. Les autres motifs, en revanche, autorisent le traitement – sous réserve de garanties – dans des situations où, indépendamment du consentement, il est approprié et nécessaire de traiter les données dans un certain contexte pour servir un intérêt légitime spécifique.

Les points b), c), d), et e) spécifient chacun un contexte particulier, dans lequel le traitement des données à caractère personnel peut être considéré comme légitime. Les conditions qui s'appliquent dans chacun de ces différents contextes requièrent une attention minutieuse, car elles déterminent la portée des différents motifs légitimant le traitement. Plus particulièrement, les critères du traitement «nécessaire à l'exécution d'un contrat», «nécessaire au respect d'une obligation légale», «nécessaire à la sauvegarde de l'intérêt vital de la personne concernée» et «nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique» sont assortis d'exigences différentes, qui ont été examinées à la section III.2.

[110] À propos du droit à la portabilité des données, voir l'article 18 du règlementproposé.

Le point f) fait référence, plus généralement, à un (quelconque) intérêt légitime poursuivi par le responsable du traitement (dans n'importe quel contexte). Cette disposition générale est, cependant, expressément subordonnée à un critère supplémentaire de mise en balance, qui requiert que l'intérêt légitime poursuivi par le responsable du traitement – ou par le ou les tiers auxquels les données sont communiquées – soit comparé avec les intérêts ou les droits fondamentaux des personnes concernées.

Rôle de l'article 7, point f)

L'article 7, point f), ne doit pas être perçu comme un fondement juridique pouvant uniquement être utilisé avec parcimonie pour combler certaines lacunes «en dernier ressort» dans des situations rares et imprévues, ou comme une dernière chance si aucun autre motif ne s'applique. Il ne doit pas non plus apparaître comme une option privilégiée, et il ne s'agit pas d'encourager indûment son utilisation parce qu'il serait considéré comme moins contraignant que les autres motifs. Il s'agit plutôt d'un moyen, tout aussi valable que l'un quelconque des autres motifs permettant de légitimer le traitement des données à caractère personnel.

Une utilisation appropriée de l'article 7, point f), dans les circonstances appropriées et moyennant des garanties adéquates, permet aussi d'éviter une utilisation abusive et une invocation excessive d'autres fondements juridiques. Une évaluation appropriée de l'équilibre requis par l'article 7, point f), souvent assortie d'une possibilité de s'opposer au traitement, peut, dans d'autres cas, se substituer valablement à l'invocation inappropriée, par exemple, du motif du «consentement» ou du caractère «nécessaire à l'exécution d'un contrat». Dans cette optique, l'article 7, point f), présente des garanties complémentaires par rapport aux autres motifs prédéfinis. Il ne doit donc pas être considéré comme «le maillon faible» ou comme une porte ouverte à la légitimation de tout traitement de données qui ne relève pas d'un des autres fondements juridiques.

Intérêt légitime poursuivi par le responsable du traitement / intérêt ou droits fondamentaux de la personne concernée

La notion d'«intérêt» désigne, au sens large, l'enjeu poursuivi par le responsable du traitement, ou le bénéfice qu'il tire du traitement – ou que la société pourrait en tirer. Il peut être impérieux, manifeste ou plus controversé. Les situations auxquelles renvoie l'article 7, point f), peuvent donc aller de l'exercice de droits fondamentaux ou de la protection d'intérêts personnels ou sociaux importants à d'autres contextes moins évidents, voire problématiques.

Pour être considéré comme «légitime» et pertinent au sens de l'article 7, point f), l'intérêt doit être licite, c'est-à-dire conforme au droit applicable dans l'Union et dans le pays concerné. Il doit aussi être exprimé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée. Enfin, il doit constituer un intérêt réel et présent, c'est-à-dire qu'il ne doit pas être hypothétique.

Si le responsable du traitement, ou le tiers auquel les données doivent être communiquées, poursuit un tel intérêt légitime, il ne s'ensuit pas nécessairement que l'article 7, point f), peut être invoqué comme fondement juridique justifiant le traitement. La possibilité d'invoquer l'article 7, point f), dépendra du résultat de la mise en balance qui suit. Le traitement doit aussi être «nécessaire à la réalisation de l'intérêt légitime» poursuivi par le responsable du traitement ou – en cas de communication des données – par le tiers. Des moyens plus

respectueux de la vie privée susceptibles de servir à la même finalité devraient donc toujours être préférés.

La notion d'«intérêt» des personnes concernées est définie encore plus largement, puisqu'elle n'exige pas d'élément de «légitimité». Si le responsable du traitement ou le tiers peut poursuivre n'importe quel intérêt, pour autant qu'il ne soit pas illégitime, la personne concernée devrait aussi pouvoir s'attendre à ce que ses intérêts, quelle qu'en soit la nature, soient pris en considération et mis en balance avec ceux du responsable du traitement, pour autant qu'ils soient pertinents dans le champ d'application de la directive.

Application du critère de mise en balance

Dans son interprétation du champ d'application de l'article 7, point f), le groupe de travail entend proposer une approche équilibrée, qui garantit aux responsables du traitement des données la souplesse nécessaire dans les situations où les personnes concernées ne subissent aucune incidence indue, tout en offrant aux personnes concernées une sécurité juridique et des garanties suffisantes pour empêcher un usage abusif de cette disposition ouverte.

Pour appliquer le critère de mise en balance, il importe, tout d'abord, d'examiner la nature et la source de l'intérêt légitime, ainsi que la nécessité du traitement pour la poursuite de cet intérêt, d'une part, et l'incidence sur les personnes concernées, d'autre part. Cette appréciation initiale devrait tenir compte des mesures, en matière de transparence ou de collecte limitée des données, par exemple, que le responsable du traitement prévoit d'adopter pour se conformer à la directive.

Après une analyse et un examen attentif de tous les aspects du problème, un bilan provisoire peut être établi: une conclusion préliminaire peut être tirée afin de déterminer si l'intérêt légitime poursuivi par le responsable du traitement prévaut sur les droits et les intérêts des personnes concernées. Il peut cependant y avoir des cas où le résultat de la mise en balance n'est pas clair et où il subsiste un doute quant à la question de savoir si l'intérêt légitime du responsable du traitement (ou du tiers) prévaut et si le traitement peut se fonder sur l'article 7, point f).

C'est pourquoi il importe de procéder à une évaluation complémentaire dans le cadre de l'exercice de mise en balance. À ce stade, le responsable du traitement peut envisager d'introduire d'autres mesures, qui vont au-delà du respect des dispositions horizontales de la directive, afin de contribuer à protéger les personnes concernées. Ces mesures supplémentaires peuvent comprendre, par exemple, la mise en place d'un mécanisme fonctionnel et aisément accessible garantissant aux personnes concernées la possibilité inconditionnelle de refuser le traitement.

Facteurs-clés à prendre en considération pour appliquer le critère de mise en balance

Compte tenu de ce qui précède, les facteurs qui peuvent utilement être pris en considération lors de l'application du critère de mise en balance sont:

- la nature et la source de l'intérêt légitime, et notamment:

  - si le traitement des données est nécessaire à l'exercice d'un droit fondamental, ou

- s'il est d'intérêt public à quelque autre égard ou bénéficie d'une reconnaissance sociale, culturelle ou légale/réglementaire dans la collectivité concernée;

- l'incidence sur les personnes concernées, et notamment:

  - la nature des données, comme le fait que le traitement porte ou non sur des données qui peuvent être considérées comme sensibles ou qui ont été obtenues à partir de sources publiquement accessibles;
  - la façon dont les données sont traitées, y compris si elles ont été publiées ou rendues accessibles par quelque autre moyen à un grand nombre de personnes, ou si des volumes considérables de données à caractère personnel sont traités ou combinés avec d'autres données (par exemple, en cas d'établissement de profils, à des fins commerciales, judiciaires, ou autres);
  - les attentes raisonnables de la personne concernée, en particulier à propos de l'utilisation et de la divulgation des données dans une situation donnée;
  - le statut du responsable du traitement des données et celui de la personne concernée, y compris l'équilibre des pouvoirs entre eux, ou le fait que la personne concernée soit un enfant ou appartienne à une catégorie de population plus vulnérable.

- les garanties supplémentaires destinées à prévenir toute incidence indue sur les personnes concernées, et notamment:

  - la minimisation des données (par exemple, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation);
  - les mesures techniques et organisationnelles garantissant les données ne peuvent servir à la prise de décisions ou d'autres mesures à l'endroit des individus («séparation fonctionnelle»);
  - un large recours aux techniques d'anonymisation, l'agrégation des données, les technologies renforçant la protection de la vie privée, la prise en compte du respect de la vie privée dès la conception, les analyses d'impact relatives à la vie privée et à la protection des données;
  - une transparence accrue, un droit général et inconditionnel de refuser le traitement, la portabilité des données et autres mesures connexes visant à renforcer le pouvoir des personnes concernées.

Responsabilité, transparence, droit d'opposition et au-delà

À propos de ces garanties – et de l'appréciation générale résultant de la mise en balance – trois aspects spécifiques jouent souvent un rôle crucial dans le contexte de l'article 7, point f), et requièrent donc une attention spéciale:

- l'existence de mesures supplémentaires en vue d'accroître la transparence et la responsabilité et leur nécessité éventuelle ;
- le droit de la personne concernée de s'opposer au traitement, et au-delà de cette opposition, la possibilité de refuser sans avoir à donner de justification;
- le renforcement du pouvoir des personnes concernées: portabilité des données et disponibilité de mécanismes fonctionnels permettant à la personne concernée d'accéder à ses propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur).

IV. 2. Recommandations

Le libellé actuel de l'article 7, point f), de la directive est ouvert. Cette souplesse dans sa formulation laisse une marge d'interprétation considérable et a parfois conduit – ainsi que l'expérience l'a montré – à un manque de prévisibilité et de sécurité juridique. Cependant, utilisé dans le contexte approprié, et si les critères adéquats sont appliqués, comme indiqué dans le présent avis, l'article 7, point f), a un rôle essentiel à jouer en tant que fondement juridique d'un traitement légitime des données.

Le groupe de travail soutient donc l'approche adoptée actuellement à l'article 6 de la proposition de règlement, qui maintient l'équilibre des intérêts en tant que fondement juridique séparé. D'autres orientations seraient néanmoins bienvenues pour garantir une application adéquate du critère de mise en balance.

Possibilités et moyens d'apporter des précisions

Il serait essentiel que la disposition demeure suffisamment flexible et qu'elle reflète aussi bien le point de vue du responsable du traitement des données que celui de la personne concernée, ainsi que le caractère dynamique des contextes considérés. C'est pourquoi le groupe de travail est d'avis qu'il n'est pas souhaitable de faire figurer , dans le texte du règlement proposé ou dans des actes délégués, des listes détaillées et exhaustives de situations dans lesquelles un intérêt serait, de fait, qualifié de légitime. Le groupe de travail n'est pas davantage favorable à la définition de cas où l'intérêt ou le droit d'une partie devrait *en principe* ou *par présomption* prévaloir sur l'intérêt ou le droit de l'autre partie, du simple fait de la nature de cet intérêt ou de ce droit, ou parce que certaines mesures de protection ont été prises, par exemple, parce que les données ont simplement été pseudonymisées. Cela risquerait d'être à la fois trompeur et inutilement coercitif.

Plutôt que de porter des jugements définitifs sur les mérites des différents droits et intérêts, le groupe de travail insiste sur le *rôle crucial de la mise en balance* dans l'évaluation au titre de l'article 7, point f). Il est nécessaire de conserver la flexibilité du critère, mais la façon dont il est appliqué doit être plus efficace dans la pratique et doit réellement améliorer la conformité. Cela devrait se traduire par une obligation de *responsabilité renforcée* pour les responsables du traitement des données, à qui il appartient de *démontrer* que l'intérêt et les droits de la personne concernée ne prévalent pas sur leur propre intérêt.

Orientations et responsabilité

Pour ce faire, le groupe de travail recommande, dans le règlement proposé, de formuler des orientations de la manière suivante.

1) Il serait utile d'établir et d'intégrer dans un considérant une liste non exhaustive des facteurs-clés à prendre en considération lors de l'application du critère de mise en balance, comme la nature et la source de l'intérêt légitime, l'incidence sur les personnes concernées, et les garanties supplémentaires qui peuvent être mises en place par le responsable du traitement afin de prévenir toute incidence indue sur les personnes concernées. Ces garanties peuvent comprendre, entre autres:

- une séparation fonctionnelle des données, une utilisation appropriée des techniques d'anonymisation, de chiffrement et d'autre mesures techniques et organisationnelles destinées à limiter les risques potentiels pour les personnes concernées;
- mais aussi des mesures visant à garantir aux personnes concernées une transparence accrue et une plus grande liberté de choix, comme, éventuellement, la possibilité inconditionnelle de refuser le traitement, sans frais et d'une manière qui puisse être aisément et effectivement invoquée.

2) Le groupe de travail est aussi favorable à une clarification, dans le règlement proposé, de la façon dont le responsable du traitement pourrait apporter la preuve d'un [111] renforcement de sa responsabilité.

La modification des conditions dans lesquelles les personnes concernées peuvent exercer le droit d'opposition prévu à l'article 19 du règlement proposé constitue déjà un élément important du point de vue de la responsabilité. Si la personne concernée s'oppose au traitement de ses données en vertu de l'article 7, point f), il appartiendra désormais au responsable du traitement des données, en application du règlement proposé, de démontrer que son intérêt prévaut. Le groupe de travail approuve sans réserve ce renversement de la charge de la preuve, qui contribue à une obligation renforcée de responsabilité.

Si le responsable du traitement des données ne parvient pas à démontrer à la personne concernée que son intérêt prévaut dans un cas précis, cela peut avoir des conséquences plus larges sur l'ensemble du traitement, et pas uniquement à l'égard de la personne concernée qui a manifesté son opposition. Le responsable du traitement peut être amené, le cas échéant, à remettre en question ou à réorganiser le traitement, dans l'intérêt non seulement de cette personne concernée en particulier, mais aussi de toutes les autres personnes concernées qui peuvent se trouver dans une situation similaire[112].

Cette exigence est nécessaire, mais non suffisante. Afin d'assurer dès le départ la protection des personnes concernées et d'éviter que le renversement de la charge de la preuve ne soit contourné[113], il importe de prendre des mesures *avant* que le traitement ne commence, et pas uniquement au cours des procédures d'«opposition» a posteriori.

Il est donc proposé que, dès le premier stade de toute activité de traitement, plusieurs mesures soient prises par le responsable du traitement des données. Les deux premières

[111] Une telle démonstration doit demeurer raisonnable et mettre l'accent sur le résultat plutôt que sur un processus administratif.

[112] Hormis le renversement de la charge de la preuve, le groupe de travail approuve aussi le fait que le règlement proposé n'exige plus qu'une opposition soit exprimée «pour des raisons *prépondérantes* et légitimes tenant à [l]a situation particulière [de la personne concernée]». Selon le règlement proposé, l'invocation de raisons légitimes (pas nécessairement «prépondérantes») tenant à la situation particulière de la personne concernée serait suffisante. D'ailleurs, une autre option, proposée dans le rapport final de la commission LIBE, consiste aussi à abandonner l'exigence que l'opposition se rapporte à la situation particulière de la personne concernée. Le groupe de travail est favorable à cette approche en ce sens qu'il recommande que les personnes concernées puissent tirer parti de l'une ou l'autre de ces possibilités ou des deux à la fois, le cas échéant, c'est-à-dire s'opposer au traitement du fait de leur situation particulière, ou d'une manière plus générale et, dans ce dernier cas, sans avoir à fournir une justification spécifique. Voir, en ce sens, l'amendement 114 sur l'article 19, paragraphe 1, du règlement proposé dans le rapport final de la commission LIBE.

[113] Les responsables du traitement des données, par exemple, peuvent être tentés d'éviter de démontrer au cas par cas que leur intérêt prévaut, en recourant à des formulaires de justification standard, ou à rendre fastidieux l'exercice du droit d'opposition.

mesures pourraient figurer dans un considérant du règlement proposé et la troisième dans une disposition spécifique:

- Effectuer une évaluation[114], qui comprendrait les différents stades de l'analyse présentée dans le présent avis et résumée à l'annexe 1. Le responsable du traitement devrait déterminer explicitement les intérêts en jeu qui prévalent et les raisons pour lesquelles ils prévalent sur les intérêts des personnes concernées. Cette évaluation préalable ne devrait pas être trop laborieuse et devrait rester *modulable*: elle peut se limiter aux critères essentiels si l'impact du traitement sur les personnes concernées est, à première vue, insignifiant, tandis qu'elle devrait être plus approfondie si l'équilibre paraît difficile à atteindre et requiert, par exemple, l'adoption de plusieurs garanties supplémentaires. Le cas échéant – c'est-à-dire quand une opération de traitement présente des risques spécifiques pour les droits et les libertés des personnes concernées –, il conviendrait de procéder à une analyse plus complète de l'incidence sur la vie privée et la protection des données (conformément à l'article 33 du règlement proposé), dont l'évaluation au regard de l'article 7, point f), pourrait constituer une part importante.

- Documenter cette évaluation. De même que le degré de détail dans lequel doit entrer l'évaluation est *modulable*, l'ampleur du travail de documentation devrait aussi être modulable. Cela dit, certains documents de base devraient néanmoins être disponibles dans tous les cas, sauf les plus anodins, indépendamment de l'appréciation de l'incidence du traitement sur la personne concernée. C'est sur la base de ces documents que l'évaluation du responsable du traitement peut ultérieurement être vérifiée et éventuellement contestée.

- Assurer la transparence et la visibilité de ces informations auprès des personnes concernées et d'autres parties prenantes. La transparence devrait toujours être garantie à l'égard des personnes concernées et des autorités chargées de la protection des données, mais aussi, le cas échéant, de l'opinion publique en général. Pour ce qui est des personnes concernées, le groupe de travail renvoie au projet de rapport de la

[114] Cette évaluation, comme indiqué précédemment en note de bas de page 84, ne devrait pas être confondue avec une analyse d'impact complète relative à la vie privée et à la protection des données. Il n'existe pas actuellement d'orientations globales pour les évaluations d'impact au niveau européen, bien que dans certains domaines, à savoir l'identification par radiofréquence et les compteurs intelligents, plusieurs efforts louables aient été consentis pour définir une méthodologie/un cadre (et/ou un modèle) au niveau sectoriel qui pourrait s'appliquer dans toute l'Union européenne. Voir la «proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)» et le «modèle d'analyse d'impact sur la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission». Le groupe de travail a émis plusieurs avis concernant ces deux méthodologies.
De plus, certaines initiatives ont été lancées en vue de définir une méthodologie d'analyse d'impact sur la protection des données, dont les efforts «spécifiques à un domaine» pourraient tirer profit. Voir, par exemple, le projet PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights): http://www.piafproject.eu/.
Pour des orientations formulées au niveau national, voir par exemple, la méthodologie de la CNIL:
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
et le manuel d'analyse d'impact sur la vie privée de l'ICO:
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

commission LIBE[115], qui indiquait que le responsable du traitement devrait informer la personne concernée des raisons qui le portent à croire que ses intérêts prévalent sur l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Selon le groupe de travail, ces informations devraient être communiquées aux personnes concernées conjointement avec celles que le responsable du traitement doit fournir conformément aux articles 10 et 11 de la directive actuelle (article 11 du règlement proposé). Cela permettra à la personne concernée de soulever éventuellement des objections dans un deuxième temps et au responsable du traitement de justifier au cas par cas les intérêts qui prévalent. En outre, le responsable du traitement devrait mettre la documentation sur laquelle il a fondé son évaluation à la disposition des autorités chargées de la protection des données, à la demande de ces dernières, afin de leur permettre de procéder éventuellement à une vérification et de faire appliquer leur décision, s'il y a lieu.

Le groupe de travail recommande que ces trois mesures soient explicitement incluses dans le règlement proposé selon les modalités énoncées plus haut. Ce serait un moyen de reconnaître le rôle des fondements juridiques dans l'appréciation de la légitimité et de clarifier l'importance du critère de mise en balance dans le contexte plus large des mesures de renforcement de la responsabilité et des analyses d'impact dans le nouveau cadre juridique proposé.

Le groupe de travail estime qu'il est également souhaitable de charger le comité européen de la protection des données de formuler au besoin d'autres orientations sur la base de ce cadre. Cette approche garantirait à la fois une clarté suffisante du texte et une flexibilité suffisante dans son application.

[115] Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)].

Annexe 1. Guide succinct sur les modalités d'application du critère de mise en balance visé à l'article 7, point f)

Étape 1: Évaluer quel fondement juridique peut éventuellement être retenu au titre de l'article 7, points a) à f)

Le traitement des données ne peut s'effectuer que si au moins un des six motifs – énoncés aux points a) à f) – de l'article 7 peut être retenu (des motifs différents peuvent être invoqués à différents stades de la même activité de traitement). S'il apparaît, à première vue, que l'article 7, point f), pourrait être un fondement juridique approprié, passer à l'étape 2.

Conseils pratiques:

- l'article 7, point a), s'applique uniquement si un consentement libre, informé, spécifique et indubitable a été donné; le fait qu'un individu n'ait pas marqué son opposition au traitement en vertu de l'article 14 ne doit pas être confondu avec le consentement visé à l'article 7, point a) – cependant, un mécanisme facile à utiliser et permettant de s'opposer à un traitement peut être considéré comme une garantie importante au regard de l'article 7, point f);
- l'article 7, point b), couvre le traitement nécessaire à l'exécution du contrat; le seul fait que le traitement des données soit lié au contrat ou prévu quelque part dans les clauses du contrat ne signifie pas nécessairement que ce motif puisse être retenu; le cas échéant, l'article 7, point f), peut être envisagé comme une autre option;
- l'article 7, point c), se rapporte uniquement à des obligations légales claires et spécifiques conformes aux législations de l'Union ou d'un État membre; dans le cas de lignes directrices non contraignantes (formulées, par exemple, par des organes de réglementation), ou d'une obligation légale étrangère, l'article 7, point f), doit être envisagé comme une autre option.

Étape 2: Qualifier un intérêt de «légitime» ou d'«illégitime»

Pour être considéré comme légitime, un intérêt doit remplir toutes les conditions suivantes:

- être licite (c'est-à-dire conforme au droit applicable dans l'Union et dans le pays concerné);
- être exprimé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment concret);
- constituer un intérêt réel et présent (c'est-à-dire ne pas être hypothétique).

Étape 3: Déterminer si le traitement est nécessaire à la réalisation de l'intérêt poursuivi

Pour remplir cette condition, examiner s'il existe d'autres moyens plus respectueux de la vie privée susceptibles d'atteindre la finalité du traitement et de servir l'intérêt légitime du responsable du traitement des données.

Étape 4: Établir un bilan provisoire en appréciant si les droits fondamentaux ou les intérêts de personnes concernées prévalent sur l'intérêt poursuivi par le responsable du traitement des données

- Tenir compte de la nature de l'intérêt poursuivi par le responsable du traitement (droit fondamental, autre type d'intérêt, intérêt public);

- évaluer le préjudice possible pour le responsable du traitement, les tiers ou la collectivité si le traitement des données n'est pas effectué;
- tenir compte de la nature des données (données sensibles au sens strict du terme ou dans un sens plus général?);
- prendre en considération le statut de la personne concernée (mineur, salarié, etc.) et celui du responsable du traitement (par exemple, si une entreprise occupe une position dominante sur le marché);
- tenir compte de la façon dont les données sont traitées (à grande échelle, extraction de données, établissement de profils, divulgation auprès d'un grand nombre de personnes ou publication);
- identifier les droits fondamentaux et/ou les intérêts des personnes concernées qui pourraient en subir les conséquences;
- prendre en considération les attentes raisonnables des personnes concernées;
- évaluer les incidences sur les personnes concernées et les comparer avec les avantages du traitement escomptés par le responsable du traitement des données.

Conseil pratique: Prendre en considération l'effet concret du traitement sur des individus en particulier – ne pas en faire un exercice abstrait ou hypothétique.

Étape 5: Établir un bilan final en tenant compte des garanties supplémentaires

Identifier et mettre en place des garanties supplémentaires appropriées résultant du devoir de vigilance et de diligence, comme:
- la minimisation des données (par exemple, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation);
- les mesures techniques et organisationnelles garantissant que les données ne peuvent servir à la prise de décisions ou d'autres mesures à l'endroit des individus («séparation fonctionnelle»);
- un large recours aux techniques d'anonymisation, l'agrégation des données, les technologies renforçant la protection de la vie privée, la prise en compte du respect de la vie privée dès la conception, les analyses d'impact relatives à la vie privée et à la protection des données;
- une transparence accrue, un droit général et inconditionnel de refuser le traitement, la portabilité des données et autres mesures connexes visant à renforcer le pouvoir des personnes concernées.

Conseil pratique: L'utilisation de technologies et d'approches renforçant la protection de la vie privée peut faire pencher la balance en faveur du responsable du traitement des données, tout en protégeant les personnes concernées.

Étape 6: Démontrer le respect des dispositions applicables et garantir la transparence

- Dresser un plan des étapes 1 à 5 pour justifier le traitement avant son lancement.
- Informer les personnes concernées des raisons qui portent le responsable du traitement à penser que la balance penche en sa faveur.
- Tenir la documentation à la disposition des autorités chargées de la protection des données.

Conseil pratique: Cette étape est *modulable*; le degré de détail de l'appréciation et de la documentation doit être adapté à la nature et au contexte du traitement. Ces mesures auront plus d'ampleur quand de gros volumes d'informations concernant de nombreuses personnes sont traités, d'une façon qui pourrait avoir une incidence considérable sur ces personnes. Une analyse d'impact complète relative à la vie privée et à la protection des données (conformément à l'article 33 du règlement proposé) ne sera nécessaire que lorsqu'une opération de traitement

présente des risques spécifiques pour les droits et libertés des personnes concernées. Dans ces cas, l'évaluation au regard de l'article 7, point f), pourrait devenir une part essentielle de cette analyse d'impact plus large.

Étape 7: Et si la personne concernée exerce son droit d'opposition?

- Lorsqu'il n'existe comme garantie qu'un droit d'opposition assorti de conditions [c'est ce qui est explicitement requis en vertu de l'article 14, point a), à titre de garantie minimale]: au cas où la personne concernée s'oppose au traitement, il convient de veiller à ce qu'un mécanisme approprié et convivial ait été mis en place pour réévaluer l'équilibre en ce qui concerne cet individu et cesser de traiter ses données si la réévaluation fait apparaître que son intérêt prévaut.
- Lorsqu'un droit de refus inconditionnel a été prévu à titre de garantie supplémentaire [parce qu'il est explicitement requis au titre de l'article 14, point b), ou parce que cette garantie supplémentaire est jugée nécessaire ou utile]: au cas où la personne concernée s'oppose au traitement, il convient de veiller à ce que son choix soit respecté, sans qu'il soit nécessaire de faire d'autres démarches ou de procéder à une nouvelle évaluation.

Annexe 2. Exemples pratiques destinés à illustrer l'application du critère de mise en balance visé à l'article 7, point f)

Cette annexe présente des exemples de certains des contextes les plus courants où la question de l'intérêt légitime au sens de l'article 7, point f), peut se poser. Le plus souvent, nous avons regroupé sous une même rubrique au moins deux exemples liés qu'il est intéressant de comparer. Bon nombre des exemples reposent sur des situations réelles, ou des éléments de cas réels auxquels sont confrontées les autorités chargées de la protection des données dans les différents États membres. Nous avons cependant modifié parfois les faits dans une certaine mesure pour mieux illustrer comment le critère de mise en balance doit être appliqué.

Ces exemples sont fournis pour illustrer le *processus de réflexion*: la méthode à utiliser pour tenir compte des multiples facteurs du critère de mise en balance. Autrement dit, les exemples *ne sont pas* destinés à présenter une évaluation *concluante* des situations décrites. En effet, dans beaucoup de cas, en modifiant les circonstances d'une manière ou d'une autre (par exemple, si le responsable du traitement venait à adopter des garanties supplémentaires comme une anonymisation plus complète, de meilleures mesures de sécurité et davantage de transparence ou de liberté de choix pour les personnes concernées), le résultat de la mise en balance pourrait changer[116].

Cela devrait encourager les responsables du traitement à mieux respecter l'ensemble des dispositions horizontales de la directive et à prévoir, s'il y a lieu, des mesures supplémentaires fondées sur le respect de la vie privée et la protection des données dès la conception. Plus les responsables du traitement ont soin de protéger les données à caractère personnel d'une manière générale, plus ils ont des chances de satisfaire au critère de mise en balance.

Exercice du droit à la liberté d'expression ou d'information[117], notamment dans les médias et dans les arts

Exemple 1: une ONG republie les dépenses des parlementaires

Une administration publie – en vertu d'une obligation légale [article 7, point c)] – les dépenses des parlementaires; par la suite, une ONG qui se consacre à la transparence analyse les données et les republie dans une version exacte et proportionnée, mais plus informative et annotée, afin de contribuer à renforcer la transparence et la responsabilité.

En supposant que l'ONG assure le travail de republication et d'annotation de manière fidèle et proportionnée, adopte des garanties appropriées et, plus généralement, respecte les droits des individus concernés, elle devrait pouvoir invoquer l'article 7, point f), comme fondement juridique justifiant le traitement. La nature de l'intérêt légitime (un droit fondamental à la

[116] L'application correcte de l'article 7, point f), peut donner lieu à des questions d'appréciation complexes et il peut être utile, pour éclairer l'évaluation, de s'appuyer sur une législation et une jurisprudence spécifiques, sur des lignes directrices, des codes de conduite et d'autres critères formels ou informels.

[117] À propos de la liberté d'expression ou d'information, voir la page 38 de l'avis. Les dérogations éventuelles applicables en vertu du droit national pour le traitement à des fins de journalisme, conformément à l'article 9 de la directive, doivent aussi être prises en compte dans l'appréciation de ces exemples.

liberté d'expression ou d'information), l'intérêt public servi par la transparence et la responsabilité, et le fait que les informations aient déjà été publiées et se rapportent à des données à caractère personnel (relativement moins sensibles) liées aux activités menées par des individus dans l'exercice de leurs fonctions publiques[118] sont autant de facteurs qui pèsent en faveur de la légitimité du traitement. Un autre élément contribuant à l'évaluation favorable tient à ce que la publication initiale était requise par la loi et que les personnes concernées devaient donc s'attendre à voir leurs données publiées. Dans l'autre plateau de la balance, on trouve l'incidence sur les individus qui peut être considérable, à cause du jugement du public, et la mise en cause possible de l'intégrité de certains individus pouvant entraîner, par exemple, une défaite aux élections, voire dans certains cas une enquête pénale sur des activités frauduleuses. Dans l'ensemble, les facteurs ci-dessus montrent cependant que, tout bien pesé, l'intérêt poursuivi par le responsable du traitement (et l'intérêt des citoyens à qui les données sont communiquées) prévaut sur l'intérêt des personnes concernées.

Exemple 2: un conseiller municipal prend sa fille comme assistante

Un journaliste publie un article bien documenté, relatant des faits avérés, dans un journal local en ligne, qui révèle qu'un conseiller municipal n'a assisté qu'à une seule réunion du conseil sur les onze dernières et indique qu'il a peu de chances d'être réélu en raison d'un récent scandale à propos de la nomination de sa fille, âgée de dix-sept ans, comme assistante.

Une analyse semblable à celle de l'*exemple 1* s'applique également ici. En ce qui concerne les faits, il est dans l'intérêt légitime du journal en question de publier l'information. Même si des données à caractère personnel ont été révélées à propos du conseiller, le droit de ce dernier au respect de sa vie privée ne prévaut pas sur le droit fondamental à la liberté d'expression qui justifie la publication de l'article dans le journal. Cette appréciation tient au fait que le droit des personnalités publiques en matière de vie privée est relativement limité au regard de leurs activités publiques et à l'importance particulière de la liberté d'expression – surtout si la publication des informations est d'intérêt public.

Exemple 3: un délit mineur continue à apparaître parmi les premiers résultats d'une recherche en ligne

Les archives en ligne d'un journal contiennent un article déjà ancien relatif à une personne qui a, par le passé, connu une certaine célébrité au plan local en tant que capitaine d'une petite équipe de football amateur. Cet individu est identifié par son nom complet et l'article porte sur une procédure pénale relativement mineure le concernant (ivresse et trouble à l'ordre public). Le casier judiciaire de cet homme est aujourd'hui vierge et l'ancien délit pour lequel il a purgé sa peine voici plusieurs années n'y figure plus. Ce qui est gênant pour cet individu, c'est que lorsqu'une recherche sur son nom est effectuée avec les principaux moteurs de recherche en ligne, les premiers résultats affichés font apparaître le lien vers ce vieil article le concernant. Malgré une demande introduite par la personne concernée, le journal refuse de prendre des mesures techniques qui restreindraient la disponibilité générale de l'article qui lui

[118] Il ne peut être exclu que certaines dépenses révèlent des données plus sensibles, touchant à la santé, par exemple. Si tel est le cas, il conviendrait de les effacer de l'ensemble de données avant la première publication. Une bonne pratique consiste à adopter une «démarche proactive» et à offrir aux personnes concernées l'occasion d'examiner leurs données avant toute publication, en les informant clairement des possibilités et des modalités de publication.

est consacré. Par exemple, le journal n'envisage pas d'adopter des mesures techniques et organisationnelles qui viseraient – dans la mesure où la technologie le permet – à limiter l'accès aux informations à partir de moteurs de recherche externes qui se servent du nom de la personne comme critère de recherche.

C'est là un autre cas illustrant le conflit possible entre la liberté d'expression et le droit au respect de la vie privée. Cela montre aussi que, parfois, des garanties supplémentaires – comme le fait de veiller à ce que, au moins en cas d'opposition justifiée en vertu de l'article 14, point a), de la directive, la partie concernée des archives du journal ne soit plus accessible par des moteurs de recherche externes ou le format utilisé pour afficher les informations ne permette plus de recherches sur le nom – peuvent jouer un rôle essentiel pour trouver un équilibre adéquat entre les deux droits fondamentaux en cause. Cela ne fait pas obstacle à d'autres mesures éventuelles qui pourraient être prises par les moteurs de recherche ou d'autres tiers[119].

Prospection directe conventionnelle et autres formes de prospection commerciale ou de publicité

Exemple 4: un magasin d'informatique envoie à ses clients des publicités pour des produits similaires

Un magasin d'informatique obtient de ses clients leurs coordonnées de contact dans le cadre de la vente d'un produit et se sert de ces coordonnées à des fins de prospection par courrier ordinaire pour promouvoir ses propres produits similaires. Le magasin vend aussi des produits en ligne et envoie des courriers électroniques promotionnels quand une nouvelle gamme de produits entre en stock. Les clients disposent d'informations claires sur la possibilité qu'ils ont de s'y opposer, sans frais et de manière simple, quand leurs coordonnées de contact sont collectées et chaque fois qu'un message est envoyé, au cas où ils n'auraient pas refusé initialement.

La transparence du traitement, le fait que le client peut raisonnablement s'attendre à recevoir des offres pour des produits similaires en tant que client du magasin et le droit d'opposition contribuent à renforcer la légitimité du traitement et à garantir les droits des individus. Dans l'autre plateau de la balance, il ne semble pas y avoir d'incidence disproportionnée sur le droit au respect de la vie privée (dans cet exemple, nous avons supposé que le magasin d'informatique n'établit pas de profils complexes de ses clients, en se servant, par exemple, d'une analyse détaillée de ses données de consultation en ligne).

Exemple 5: une pharmacie en ligne établit des profils détaillés

Une pharmacie en ligne se livre à des activités de prospection fondées sur les achats de médicaments et autres produits faits par ses clients, y compris des produits obtenus avec une prescription médicale. Elle analyse ces informations – combinées à des données démographiques à propos de sa clientèle, par exemple l'âge et le sexe – afin d'établir un «profil de santé et de bien-être» de chaque client. Le profil utilise des données de l'historique de navigation, qui sont collectées non seulement à propos des produits achetés par les clients,

[119] Voir aussi l'affaire C-131/12 Google Spain/Agencia Española de Proteccion de Datos, actuellement pendante devant la Cour de justice de l'Union européenne.

mais aussi à propos des produits et des informations qu'ils ont consultés sur le site internet. Les profils de clients comprennent des informations ou des prévisions indiquant qu'une cliente est enceinte, qu'une autre souffre d'une maladie chronique particulière, ou serait intéressée par l'achat de compléments alimentaires, de lotion solaire ou d'autres produits de soin de la peau à certaines périodes de l'année. Les analystes de la pharmacie en ligne se servent de ces informations pour envoyer à certaines personnes des courriers électroniques leur proposant des médicaments vendus sans prescription, des compléments alimentaires et d'autres produits. Dans ce cas, la pharmacie ne peut invoquer son intérêt légitime pour justifier la création et l'utilisation de profils de ses clients à des fins de prospection. L'activité de profilage décrite pose plusieurs problèmes. Les informations sont particulièrement sensibles et peuvent révéler beaucoup de choses sur des sujets qui sont censés rester privés aux yeux de la plupart des individus[120]. L'ampleur de cette activité de profilage et la manière dont elle est effectuée (utilisation de l'historique de navigation, algorithmes prédictifs) révèlent aussi un degré élevé d'ingérence dans la vie privée. Un consentement fondé sur l'article 7, point a), et sur l'article 8, paragraphe 2, point a) (lorsqu'il s'agit de données sensibles) pourrait cependant, si besoin est, constituer une autre option.

Messages non commerciaux non sollicités, notamment à des fins de campagne politique ou de collecte de fonds pour des actions caritatives

Exemple 6: une candidate aux élections locales fait un usage ciblé de la liste électorale

Une candidate aux élections locales se sert de la liste électorale[121] pour envoyer une lettre de présentation à chaque électeur potentiel de sa circonscription dans le cadre de sa campagne pour les prochaines élections. La candidate n'utilise les données obtenues dans la liste électorale que pour envoyer sa lettre et ne conserve pas les données après la fin de la campagne.

Cette utilisation du registre local s'inscrit dans les attentes raisonnables des individus, quand elle intervient au cours de la période préélectorale: l'intérêt de la responsable du traitement est clair et légitime. L'usage limité et ciblé des informations contribue aussi à faire pencher la balance en faveur de l'intérêt légitime de la responsable du traitement. Une telle utilisation des listes électorales peut aussi être réglementée par la loi au niveau national, dans une perspective d'intérêt public, de façon à prévoir des règles spécifiques, des limitations et des garanties. Si tel est le cas, le respect de ces règles spécifiques est également requis afin de garantir la légitimité du traitement.

Exemple 7: une association sans but lucratif collecte des informations à des fins d'envois de messages ciblés

[120] Au-delà des restrictions éventuelles imposées par les lois en matière de protection des données, la publicité pour des produits soumis à prescription médicale est aussi strictement réglementée dans l'Union, et il existe certaines restrictions concernant la publicité pour les médicaments vendus sans prescription. Par ailleurs, les exigences de l'article 8 à propos des catégories particulières de données (comme les données relatives à la santé) doivent aussi être prises en considération.

[121] Il est supposé que dans l'État membre où l'exemple s'applique, une liste électorale est établie en vertu de la loi.

Une organisation philosophique qui se consacre au développement humain et social décide de mener des actions de collecte de fonds organisées sur la base du profil de ses membres. À cette fin, elle collecte des données sur les sites de réseaux sociaux au moyen d'un logiciel spécialement conçu pour cibler les individus qui ont «aimé» la page de l'organisation, «aimé» ou «partagé» les messages postés par l'organisation sur sa page, consulté régulièrement certains sujets ou re-tweeté les messages de l'organisation. Elle envoie ensuite des messages et des lettres d'information à ses membres en fonction de leurs profils. Par exemple, les personnes âgées qui ont un chien et qui ont «aimé» des articles sur les refuges pour animaux reçoivent des appels aux dons différents de ceux adressés aux familles avec enfants en bas âge; les personnes appartenant à des groupes ethniques différents reçoivent aussi des messages différents.

Le fait que des catégories particulières de données soient traitées (convictions philosophiques) requiert le respect de l'article 8, une condition qui paraît être remplie puisque le traitement est effectué dans le cadre des activités légitimes de l'organisation. Ce n'est cependant pas une condition suffisante dans ce cas: la façon dont les données sont utilisées excède les attentes raisonnables des individus. Le volume de données collectées, le manque de transparence à propos de la collecte et la réutilisation de données communiquées initialement à une fin différente contribuent à la conclusion que l'article 7, point f), ne peut pas être invoqué en l'occurrence. Le traitement ne doit donc pas être autorisé, à moins qu'un autre motif puisse être invoqué, par exemple le consentement des personnes concernées donné conformément à l'article 7, point a).

Exécution de demandes en justice, y compris le recouvrement de créances via des procédures extrajudiciaires

Exemple 8: litige à propos de la qualité de travaux de rénovation

Un client conteste la qualité de travaux de rénovation réalisés dans sa cuisine et refuse de payer la totalité du prix demandé. L'entrepreneur transmet des données pertinentes et proportionnées à son avocat pour lui permettre d'envoyer un rappel au client et de négocier un arrangement avec lui s'il continue à refuser de payer.

Dans ce cas, les démarches préliminaires accomplies par l'entrepreneur au moyen d'informations de base sur la personne concernée (par exemple, nom, adresse, référence du contrat) pour lui envoyer un rappel (directement ou, en l'occurrence, par l'intermédiaire de son avocat) peuvent encore relever du traitement nécessaire à l'exécution du contrat [article 7, point b)]. Les étapes suivantes[122], incluant l'intervention d'une société de recouvrement de créances, devraient cependant être appréciées au regard de l'article 7, point f), compte tenu, entre autres, du degré d'ingérence et de l'incidence sur la personne concernée, comme on le verra dans l'exemple suivant.

Exemple 9: un client disparaît avec une voiture achetée à crédit

[122] Selon les États membres, il existe actuellement un certain degré de variabilité quant aux mesures qui peuvent être jugées nécessaires à l'exécution d'un contrat.

Un client cesse de payer les mensualités dues pour l'achat à crédit d'une coûteuse voiture de sport et «disparaît» ensuite. Le concessionnaire fait appel à un «agent de recouvrement» tiers. L'agent de recouvrement mène une enquête intrusive «de type judiciaire», en recourant notamment à la vidéosurveillance avec camera cachée et à des écoutes téléphoniques.

Bien que l'intérêt poursuivi par le concessionnaire et par l'agent de recouvrement soit légitime, la balance ne penche pas en leur faveur à cause des méthodes intrusives utilisées pour collecter des informations, dont certaines sont explicitement interdites par la loi (écoutes téléphoniques). La conclusion serait différente si, par exemple, le concessionnaire ou l'agent de recouvrement n'avaient effectué que des vérifications limitées pour confirmer les coordonnées de contact de la personne concernée afin d'engager des poursuites en justice.

Prévention de la fraude, de l'utilisation abusive de services, ou du blanchiment d'argent

Exemple 10: vérification des données des clients avant l'ouverture d'un compte bancaire

Une institution financière suit des procédures raisonnables et proportionnées – conformément aux lignes directrices non contraignantes de l'autorité publique de surveillance financière compétente – afin de vérifier l'identité de toute personne qui souhaite ouvrir un compte. Elle conserve dans ses archives les informations utilisées pour vérifier l'identité de la personne.

L'intérêt poursuivi par le responsable du traitement est légitime et le traitement des données porte uniquement sur des informations limitées et nécessaires (pratique normale dans ce secteur d'activités, à laquelle s'attendent raisonnablement les personnes concernées, et recommandée par les autorités compétentes). Des garanties appropriées ont été mises en place pour limiter toute incidence indue et disproportionnée sur les personnes concernées. Le responsable du traitement peut donc invoquer l'article 7, point f). Sinon, et dans la mesure où les procédures utilisées sont spécifiquement requises par le droit en vigueur, l'article 7, point c), pourrait s'appliquer.

Exemple 11: échange d'informations pour lutter contre le blanchiment d'argent

Une institution financière – après avoir obtenu l'avis de l'autorité compétente chargée de la protection des données – met en place des procédures fondées sur des critères spécifiques et limités pour échanger avec d'autres filiales du même groupe des données relatives à un contournement présumé des règles de lutte contre le blanchiment d'argent, en prévoyant des limitations d'accès strictes, des mesures de sécurité et une interdiction de toute utilisation ultérieure à d'autres fins.

Pour des raisons semblables à celles exposées ci-dessus, et selon les circonstances, le traitement des données pourrait être fondé sur l'article 7, point f). Sinon, et dans la mesure où les procédures appliquées sont spécifiquement requises par le droit en vigueur, l'article 7, point c), pourrait s'appliquer.

Exemple 12: liste noire de toxicomanes agressifs

Un groupe d'hôpitaux crée une liste noire commune d'individus «agressifs» qui cherchent à se procurer des médicaments, afin de leur interdire l'accès aux locaux des hôpitaux participants.

Même si l'intérêt des responsables du traitement à assurer la sécurité des hôpitaux est légitime, il doit être mis en balance avec le droit fondamental au respect de la vie privée et avec d'autres considérations impératives comme la nécessité de ne pas priver les individus concernés d'un accès à des soins médicaux. Le fait que le traitement porte sur des données sensibles (par exemple, des données médicales relatives à une toxicomanie) corrobore aussi la conclusion que, dans ce cas, il est peu probable que le traitement puisse être justifié en vertu de l'article 7, point f)[123]. Le traitement pourrait être acceptable s'il était, par exemple, encadré par une loi prévoyant des garanties spécifiques (vérifications et contrôles, transparence, prévention des décisions automatisées) pour faire en sorte qu'il n'entraîne pas de discrimination ou de violation des droits fondamentaux des individus[124]. Dans ce dernier cas, selon que cette législation spécifique requiert ou autorise seulement le traitement, soit l'article 7, point c), soit l'article 7, point f), pourrait être invoqué comme fondement juridique.

Surveillance du personnel à des fins de sécurité ou de gestion

Exemple 13: utilisation des heures de travail des avocats à des fins de facturation et de calcul de primes

Le nombre d'heures facturables accomplies par les membres d'un cabinet d'avocats est traité à la fois à des fins d'établissement des factures et pour la détermination des primes annuelles. Le système est expliqué de manière transparente aux employés qui disposent d'un droit explicite de marquer leur désaccord avec les conclusions en ce qui concerne tant la facturation que le paiement des primes, ce qui donne alors lieu à des discussions avec la direction.

Le traitement paraît nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement et il ne semble pas qu'il existe un moyen plus respectueux de la vie privée susceptible de servir à la même finalité. L'incidence sur les employés est d'ailleurs limitée, grâce aux garanties et aux processus mis en place. L'article 7, point f), pourrait donc constituer un fondement juridique approprié dans ce cas. Il pourrait aussi être soutenu que le traitement effectué à l'une de ces fins ou aux deux est nécessaire à l'exécution du contrat.

[123] Les exigences de l'article 8 à propos des catégories particulières de données (comme les données de santé) doivent aussi être prises en considération.

[124] Voir le document de travail sur les listes noires (WP 65), adopté le 3 octobre 2002.

Exemple 14: surveillance électronique de l'utilisation de l'internet[125]

Un employeur surveille l'utilisation de l'internet par les salariés durant les heures de travail pour s'assurer qu'ils ne font pas un usage personnel excessif de l'équipement informatique de la société. Les données collectées comprennent les fichiers temporaires et les cookies créés sur les ordinateurs des salariés, l'historique des sites visités et des téléchargements effectués durant les heures de travail. Les données sont traitées sans consultation préalable des personnes concernées ni des représentants syndicaux/du comité d'entreprise. Les informations fournies aux individus concernés à propos de ces pratiques sont insuffisantes.

Le volume et la nature des données collectées représentent une ingérence considérable dans la vie privée des salariés. En plus des questions de proportionnalité, la transparence des pratiques, étroitement liée aux attentes raisonnables des personnes concernées, est aussi un facteur important à prendre en considération. Même si l'employeur a un intérêt légitime à limiter le temps consacré par les salariés à visiter des sites internet qui ne sont pas directement pertinents pour leur travail, les méthodes utilisées ne satisfont pas au critère de mise en balance prévu par l'article 7, point f). L'employeur devrait recourir à des méthodes moins intrusives (par exemple, limiter l'accessibilité de certains sites), qu'il conviendrait, pour se conformer aux meilleures pratiques, de discuter et d'approuver conjointement avec les représentants du personnel et de communiquer aux salariés de façon transparente.

Mécanismes de dénonciation des dysfonctionnements

Exemple 15: mécanisme de dénonciation des dysfonctionnements répondant à des obligations légales étrangères

Une filiale européenne d'un groupe américain met en place un mécanisme limité de dénonciation des dysfonctionnements pour signaler les infractions graves dans le domaine de la comptabilité et des finances. Les entités du groupe sont soumises à un code de bonne gouvernance qui préconise un renforcement des procédures de contrôle interne et de gestion des risques. Du fait de ses activités internationales, la filiale européenne est tenue de fournir des données financières fiables aux autres membres du groupe aux États-Unis. Le mécanisme est conçu pour être conforme au droit américain et aux lignes directrices formulées par les autorités nationales chargées de la protection des données dans l'Union.

Parmi les garanties prévues, des séances de formation ainsi que d'autres moyens servent à donner des orientations claires aux salariés sur les circonstances dans lesquelles il convient d'utiliser le mécanisme. Le personnel est mis en garde contre tout abus – par exemple, des allégations fausses ou sans fondement à l'encontre de collègues. Il est aussi expliqué aux salariés qu'ils peuvent, à leur convenance, utiliser le mécanisme de façon anonyme ou en s'identifiant. Dans ce dernier cas, ils sont avisés des circonstances dans lesquelles les informations qui les identifient seront transmises à leur employeur ou à d'autres agences.

Si le droit européen ou la législation d'un État membre de l'Union exigeait la mise en place du mécanisme, le traitement pourrait se fonder sur l'article 7, point c). Cependant, les

[125] Quelques États membres estiment qu'un contrôle électronique limité peut être «nécessaire à l'exécution d'un contrat» et peut donc tirer son fondement juridique de l'article 7, point b), plutôt que de l'article 7, point f).

obligations légales étrangères ne sont pas considérées comme une obligation légale au sens de l'article 7, point c), et ne peuvent donc pas servir à légitimer le traitement en vertu de l'article 7, point c). Le traitement pourrait néanmoins se fonder sur l'article 7, point f), par exemple, s'il existe un intérêt légitime à garantir la stabilité des marchés financiers ou à lutter contre la corruption, et pour autant que le mécanisme comporte des garanties suffisantes, conformément aux orientations des autorités de réglementation compétentes dans l'Union.

Exemple 16: mécanisme interne de dénonciation des dysfonctionnements dépourvu de procédures cohérentes

Une société de services financiers décide d'instaurer un mécanisme de dénonciation des dysfonctionnements parce qu'elle soupçonne l'existence de pratiques répandues de détournement et de corruption parmi son personnel et souhaite encourager les salariés à se surveiller mutuellement. Dans un souci d'économie, la société décide d'intégrer le mécanisme à son fonctionnement interne, en confiant sa gestion aux membres de son service de ressources humaines. Pour inciter les salariés à faire usage du mécanisme, elle offre une gratification en espèces «en toute discrétion» à ceux dont la contribution permet de repérer des conduites inappropriées et de recouvrer des fonds.

La société a sans doute un intérêt légitime à détecter et prévenir le vol et la corruption. Cependant, son mécanisme de dénonciation des dysfonctionnements est si mal conçu et dépourvu de garanties que l'intérêt et le droit au respect de la vie privée des salariés prévalent – en particulier de ceux qui pourraient être victimes de fausses accusations formulées dans le seul but d'un gain financier. Le fait que le mécanisme soit géré en interne plutôt que de manière indépendante pose un autre problème, tout comme le manque de formation et d'orientations concernant l'utilisation du mécanisme.

Sécurité physique, sécurité des systèmes et réseaux informatiques

Exemple 17: contrôles biométriques dans un laboratoire de recherche

Un laboratoire de recherche scientifique travaillant sur des virus mortels utilise un système d'accès biométrique en raison du risque élevé pour la santé publique au cas où ces virus viendraient à sortir des installations. Des garanties appropriées sont appliquées, notamment la conservation des données biométriques sur des cartes personnelles que les salariés gardent en leur possession plutôt que dans un système centralisé.

Même si les données sont sensibles, au sens large du terme, leur traitement est motivé par des raisons d'intérêt public. Ces considérations, ajoutées au fait que les risques d'abus sont réduits par le recours à des garanties appropriées, font de l'article 7, point f), une base juridique adéquate justifiant le traitement.

Exemple 18: caméras cachées servant à identifier les visiteurs et les salariés qui fument

Une société utilise des caméras cachées pour identifier les visiteurs et les salariés qui fument dans des locaux du bâtiment où ce n'est pas autorisé.

Bien que le responsable du traitement ait un intérêt légitime à veiller au respect de l'interdiction de fumer, les moyens utilisés à cet effet sont, d'une manière générale,

disproportionnés et inutilement intrusifs. Il existe des méthodes plus respectueuses de la vie privée et plus transparentes (comme les détecteurs de fumée et les panneaux d'interdiction visibles). Le traitement n'est donc pas conforme à l'article 6, qui requiert que les données soient «non excessives» au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. De même, il ne satisfera probablement pas au critère de mise en balance visé à l'article 7.

Recherche scientifique

Exemple 19: recherches relatives aux effets du divorce et du chômage des parents sur la réussite scolaire des enfants

Dans le cadre d'un programme lancé par le gouvernement et autorisé par un comité d'éthique compétent, des recherches sont menées sur la relation entre le divorce, le chômage des parents et la réussite scolaire des enfants. Sans faire partie des «catégories particulières de données», l'objet de ces recherches tient néanmoins à des questions qui, pour de nombreuses familles, seraient considérées comme personnelles et très intimes. Les recherches permettront de mettre en place une assistance pédagogique spéciale ciblant des enfants qui seraient exposés, sinon, à des risques d'absentéisme, de mauvais résultats scolaires et, parvenus à l'âge adulte, de chômage et de criminalité. La législation de l'État membre concerné autorise explicitement le traitement des données à caractère personnel (à l'exception des catégories particulières de données) à des fins de recherches, pour autant que ces travaux soient nécessaires à la réalisation d'un intérêt public important et menés dans le respect de garanties adéquates, qui sont décrites en détail dans des dispositions d'exécution. Ce cadre juridique inclut des exigences spécifiques, mais aussi une structure de responsabilité qui permet l'évaluation au cas par cas de l'admissibilité des recherches (si elles sont effectuées sans le consentement des individus concernés) et des mesures à appliquer en particulier pour protéger les personnes concernées.

Le chercheur dirige un centre de recherche sûr auquel sont transmises les informations pertinentes, dans des conditions sécurisées, par le registre de population, les tribunaux, les services d'aide à l'emploi et les écoles. Le centre de recherche procède alors au «hachage» des identités individuelles pour que les enregistrements relatifs aux divorces, au chômage et aux résultats scolaires puissent être liés sans révéler les identités «civiles» des individus – par exemple, leurs noms et leurs adresses. Toutes les données originales sont ensuite définitivement supprimées. D'autres mesures sont prises pour assurer la séparation fonctionnelle (c'est-à-dire garantir que les données serviront uniquement à des fins de recherche) et réduire le risque de ré-identification éventuelle.

Les membres du personnel qui travaillent au centre de recherche reçoivent une formation rigoureuse en matière de sécurité et sont personnellement responsables – voire passibles de poursuites pénales – pour tout manquement à la sécurité qui leur serait imputable. Des mesures techniques et organisationnelles sont prises, par exemple, pour garantir que les employés qui se servent de clés USB ne peuvent pas faire sortir des données à caractère personnel du centre.

Le centre de recherche a un intérêt légitime à effectuer ces travaux, qui présentent un grand intérêt public. Lesdits travaux sont aussi dans l'intérêt légitime des administrations de l'emploi, de l'éducation et d'autres organismes participant au programme, qui seront mieux à même de planifier et dispenser des services à ceux qui en ont le plus besoin. Les aspects du

programme touchant à la vie privée ont été bien conçus et les garanties mises en place font que ni l'intérêt ni le droit au respect de la vie privée des parents ou des enfants dont les données ont servi de base aux recherches ne prévalent sur l'intérêt légitime des organisations qui mènent ces travaux.

Exemple 20: étude sur l'obésité

Une université souhaite mener des recherches sur les niveaux d'obésité infantile dans plusieurs villes et collectivités rurales. Malgré les difficultés auxquelles elle se heurte généralement pour obtenir des écoles et autres institutions un accès aux données pertinentes, elle parvient à convaincre quelques dizaines d'enseignants à suivre pendant un certain temps les enfants de leurs classes qui paraissent obèses et à leur poser des questions à propos de leurs habitudes alimentaires, de leurs niveaux d'activité physique, du temps qu'ils consacrent à jouer à des jeux vidéo, etc. Ces enseignants consignent aussi les noms et adresses des enfants interrogés pour leur faire envoyer un coupon permettant de télécharger gratuitement de la musique en ligne en guise de remerciement pour leur participation. Les chercheurs constituent ensuite une base de données sur les enfants, en mettant en corrélation les niveaux d'obésité avec l'activité physique et d'autres facteurs. Les exemplaires papier des questionnaires complétés – sous une forme qui permet encore d'identifier les enfants – sont conservés dans les archives de l'université pendant une durée indéterminée, sans mesures de sécurité adéquates. Des photocopies de tous les questionnaires sont envoyées sur demande à tout étudiant de la faculté de médecine ou d'universités partenaires dans le monde entier qui manifeste son intérêt en vue d'une utilisation ultérieure des données de recherche.

Bien que l'université ait un intérêt légitime à effectuer ces recherches, la façon dont celles-ci sont conçues signifie que, à plusieurs égards, les intérêts des enfants et leurs droits au respect de la vie privée l'emportent sur cet intérêt légitime. Hormis la méthodologie, qui manque de rigueur scientifique, le problème vient en particulier de l'absence d'approche renforçant la protection de la vie privée dans la conception des recherches et de la facilité d'accès aux données à caractère personnel collectées. À aucun moment, les données des enfants ne sont codées ou anonymisées et aucune autre mesure n'a été prise pour en garantir la sécurité ou assurer une séparation fonctionnelle. Il n'a pas non plus été obtenu de consentement valide au regard de l'article 7, point a), et de l'article 8, paragraphe 2, point a), et rien n'indique qu'on ait expliqué aux enfants ou à leurs parents à quoi allaient servir leurs données à caractère personnel ou avec qui elles seraient partagées.

Obligation légale étrangère

Exemple 21: respect des exigences du droit fiscal en vigueur dans un pays tiers

Des banques de l'Union collectent et transfèrent certaines données de leurs clients aux fins du respect des obligations en matière de fiscalité qui s'appliquent à leurs clients dans un pays tiers. La collecte et le transfert de ces données sont prévus dans les conditions et garanties convenues entre l'Union et le pays étranger dans le cadre d'un accord international et s'effectuent conformément aux termes de cet accord.

Si une obligation étrangère n'est pas, en soi, considérée comme une base légitimant le traitement au titre de l'article 7, point c), elle peut le devenir dès lors qu'elle est confirmée par un accord international. Dans ce dernier cas, le traitement pourrait être jugé nécessaire au respect d'une obligation légale intégrée au cadre juridique intérieur par l'accord international.

Cependant, s'il n'existe pas d'accord de ce type, la collecte et le transfert devront faire l'objet d'une évaluation au regard des exigences de l'article 7, point f), et ne pourront être considérés comme admissibles que si des garanties adéquates sont mises en place, comme celles approuvées par l'autorité compétente chargée de la protection des données (voir aussi l'*exemple 15*, ci-dessus).

Exemple 22: transfert de données sur des dissidents

Une entreprise de l'Union transfère des données relatives à des résidents étrangers à la demande d'un régime autoritaire dans un pays tiers qui souhaite accéder aux données de dissidents (par exemple, les données relatives à leurs échanges de courriers électroniques, le contenu de ces courriers, l'historique de navigation ou des messages privés échangés sur les réseaux sociaux).

Dans ce cas, à la différence de l'exemple précédent, il n'existe aucun accord international qui autoriserait l'application de l'article 7, point c), comme fondement juridique. En outre, plusieurs éléments plaident contre une invocation de l'article 7, point f), pour justifier le traitement. Bien que le responsable du traitement puisse avoir un intérêt économique à se plier aux demandes d'un gouvernement étranger (à défaut de quoi il pourrait faire l'objet d'un traitement moins favorable de la part de l'administration du pays tiers par rapport à d'autres entreprises), la légitimité et la proportionnalité du transfert sont hautement contestables au regard du cadre des droits fondamentaux de l'Union. L'impact potentiellement gigantesque sur les individus concernés (par exemple, discrimination, emprisonnement, condamnation à mort) fait aussi pencher fortement la balance en faveur des intérêts et des droits des personnes concernées.

Réutilisation de données publiquement disponibles

Exemple 23: classement de personnalités politiques[126]

Une ONG qui se consacre à la transparence se sert de données publiquement disponibles concernant des élus (promesses faites à l'époque de leur élection et participation effective aux scrutins de l'assemblée où ils siègent) pour les classer selon le respect de leurs engagements.

Même si l'incidence sur les personnalités politiques concernées peut être considérable, le fait que le traitement se fonde sur des informations publiques et se rapporte à leurs responsabilités publiques, ajouté à une finalité évidente de renforcement de la transparence et de la responsabilité, fait pencher la balance en faveur de l'intérêt du responsable du traitement[127].

Enfants et autres personnes vulnérables

Exemple 24: site internet d'information à l'intention des adolescents

[126] Voir aussi, pour comparaison, l'*exemple 7* ci-dessus.

[127] Comme dans les *exemples 1 et 2*, nous avons supposé que la publication est exacte et proportionnée. L'absence de garanties et d'autres facteurs peuvent modifier l'équilibre des intérêts selon les circonstances.

Le site internet d'une ONG qui dispense des conseils aux adolescents sur des questions comme la drogue, la grossesse non désirée et la consommation d'alcool collecte des données via son propre serveur à propos des visiteurs du site. Ces données sont immédiatement anonymisées et transformées en statistiques générales sur les sections les plus populaires du site auprès des visiteurs selon les différentes régions géographiques du pays.

L'article 7, point f), pourrait servir de fondement juridique, même si des données concernant des individus vulnérables sont concernées, dès lors que le traitement est effectué dans l'intérêt public et que des garanties strictes ont été mises en place (les données sont immédiatement rendues anonymes et utilisées seulement pour la production de statistiques), ce qui contribue à faire pencher la balance en faveur du responsable du traitement.

Solutions de prise en compte du respect de la vie privée dès la conception utilisées comme garantie supplémentaire

Exemple 25: accès aux numéros de téléphone mobile des utilisateurs et non-utilisateurs d'une application: «comparer et oublier»

Les données à caractère personnel d'individus sont traitées pour vérifier s'ils ont déjà indubitablement donné leur consentement dans le passé (système «comparer et oublier» mis en place à titre de garantie).

Le développeur d'une application est tenu d'obtenir le consentement indubitable des personnes concernées pour traiter leurs données à caractère personnel: c'est le cas, par exemple, s'il souhaite accéder à tout le carnet d'adresses électroniques des utilisateurs de l'application, y compris les numéros de téléphone mobiles de contacts qui n'utilisent pas l'application. Pour ce faire, il peut d'abord vérifier si les détenteurs des numéros de téléphone mobile figurant dans le carnet d'adresses des utilisateurs de l'application ont déjà indubitablement donné leur consentement [conformément à l'article 7, point a)] pour le traitement de leurs données.

Pour ce traitement initial limité (à savoir, un accès en lecture à court terme à tout le carnet d'adresses de l'utilisateur d'une application), le développeur peut invoquer l'article 7, point f), comme fondement juridique, sous réserve de garanties appropriées. Ces garanties devraient inclure des mesures techniques et organisationnelles pour faire en sorte que cet accès serve uniquement à aider l'utilisateur à identifier quels sont, parmi ses contacts, ceux qui sont déjà des utilisateurs et qui ont donc déjà indubitablement donné leur consentement pour que la société collecte et traite leurs numéros de téléphone à cet effet. Les numéros de téléphone mobile des non-utilisateurs ne peuvent être utilisés et collectés que dans le but strictement limité de vérifier s'ils ont déjà indubitablement donné leur consentement et devraient être effacés immédiatement après.

Combinaison d'informations personnelles recueillies par des services internet

Exemple 26: combinaison d'informations personnelles recueillies par différents services internet

La politique de confidentialité d'une société proposant divers services sur l'internet, dont un moteur de recherche, le partage de vidéos et un réseau social, contient une clause qui l'autorise à «combiner toutes les informations personnelles» collectées à propos de chacun de

ses utilisateurs pour les différents services qu'ils utilisent, sans déterminer aucune période de conservation des données. Selon cette société, le but est de «garantir la meilleure qualité de service possible».

La société met certains outils à la disposition de différentes catégories d'utilisateurs pour leur permettre d'exercer leurs droits (par exemple, désactiver les publicités ciblées, s'opposer à l'ajout d'un type de cookies spécifique).

Cependant, les outils disponibles ne permettent pas aux utilisateurs d'exercer un contrôle effectif sur le traitement de leurs données: les utilisateurs ne peuvent pas contrôler les combinaisons spécifiques de leurs données collectées par différents services et ils ne peuvent pas s'opposer à la combinaison des données les concernant. Dans l'ensemble, il existe un déséquilibre entre l'intérêt légitime de la société et la protection des droits fondamentaux des utilisateurs, de telle sorte que l'article 7, point f), ne devrait pas pouvoir servir de fondement juridique justifiant le traitement. L'article 7, point a), constituerait un fondement plus approprié, pour autant que les conditions d'un consentement valide soient remplies.