Réflexions autour de la Protection des Données et des Vulnérabilités

Herveg, Jean

Published in:
Vulnérabilités et droits dans l'environnement numérique

Publication date:
2018

Document Version
le PDF de l'éditeur

CHAPITRE 10
Réflexions autour de la Protection des Données et des Vulnérabilités

Jean HERVEG[1]

L'idée poursuivie par la présente contribution est de passer en revue les risques auxquels les technologies de l'information et de la communication exposent les individus (I) et ensuite fournir une introduction aux mécanismes de défense mis en place par le droit de la protection des données, afin de nourrir le débat sur les vulnérabilités dans la société de l'information.

SECTION 1. – La protection des données : une protection contre les risques liés aux traitements de données à caractère personnel

1. Le droit de la protection des données ou, de manière plus précise, le droit de la protection des personnes à l'égard des traitements de données à caractère personnel, est une discipline qui étudie les dispositions juridiques à prendre pour protéger les droits et libertés des individus face au développement de technologies (ce sont les technologies de l'information et de la communication) qui permettent l'exploitation (le traitement) d'informations qui se rapportent à des personnes physiques identifiées ou identifiables (ce sont les données à caractère personnel et les personnes concernées) afin de protéger, en particulier, leur droit au respect de la vie privée. En effet, dès le début, la protection des données s'est développée

[1] UNamur, Faculté de Droit, Centre de recherche Information, Droit & Société et avocat au barreau de Bruxelles. This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreement 730953 (Inspex) and in part by the Swiss Secretariat for Education, Research and Innovation (SERI) under Grant 16.0136 730953. La publication ne reflète que l'opinion de son auteur et la Commission européenne ne peut être tenue responsable de l'usage qui en serait fait.

à partir de l'idée [sinon du constat] que ces nouvelles technologies de l'information et de la communication étaient susceptibles de porter gravement atteinte aux droits et libertés des individus.

Ainsi, dans la Recommandation 509 (1968) du 31 janvier 1968 relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes, l'Assemblée consultative du Conseil de l'Europe[2] s'inquiétait des dangers que certains aspects des nouvelles réalisations scientifiques et technologiques pouvaient faire courir aux droits et libertés des individus[3]. Elle expliquait son intervention en raison des « (…) graves dangers que font courir aux droits de l'individu certains aspects des réalisations scientifiques et technologiques modernes (…) ». Elle était convaincue que « (…) des techniques récemment développées comme l'interception des communications téléphoniques, l'écoute clandestine, l'observation subreptice, l'usage illégitime d'études statistiques officielles et autres études semblables pour l'obtention d'informations privées et la publicité et la propagande subliminales, représentent une menace pour les droits et libertés de l'individu et, en particulier, pour le droit au respect de la vie privée que protège l'article 8 de la Convention européenne des Droits de l'Homme (…) »[4].

L'Assemblée était donc inquiète de l'usage qui pouvait être fait de nouvelles technologies en matière de collecte et d'utilisation d'informations « privées » (sans que cette dernière notion ne soit autrement définie à ce stade). Elle était aussi inquiète (et de manière fort précoce en un sens) par la possibilité offerte par ces technologies d'influencer les individus par le biais de la publicité et de la propagande subliminales[5]. Elle considérait que c'était, en particulier, le droit au respect de la vie privée des individus qui était en jeu.

C'est dans ce contexte que l'Assemblée a jugé que, dans la majorité des États membres, la loi n'offrait pas aux individus de protection suffisante contre ces procédés qui menaçaient leur droit au respect de la vie privée. Il y avait, dès lors, un risque de violation de l'article 8 de la Convention européenne des droits de l'homme[6]. Elle a alors demandé au Comité des Ministres de charger le Comité d'expert en matière de droits de l'homme de procéder à une étude à ce sujet et de faire rapport sur la question de savoir si la législation

[2] *L'Assemblée consultative* du Conseil de l'Europe n'est appelée Assemblée parlementaire du Conseil de l'Europe que depuis 1974.

[3] Voy. la Recommandation 509 (1968) relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes, adoptée le 31 janvier 1968 par l'Assemblée consultation du Conseil de l'Europe durant sa 16e séance.

[4] Voy. le considérant 3 de la Recommandation.

[5] Il s'agit d'une information absorbée par l'individu à un niveau subliminal, c'est-à-dire de manière inconsciente. De cette façon, l'individu agit sur base d'informations enregistrées dans son inconscient sans qu'il le sache. Cette manipulation des individus représente, à l'évidence, une pratique *odieuse* dans une société démocratique.

[6] Voy. le considérant 4 de la Recommandation.

nationale des États membres protégeait suffisamment le droit au respect de la vie privée contre les violations qui pouvaient être commises par l'emploi des méthodes scientifiques et techniques modernes et, si la réponse à cette question devait s'avérer négative, de formuler des recommandations tendant à une meilleure protection du droit au respect de la vie privée des individus[7]. Le résultat de ces travaux furent présentés lors d'un Colloque organisé à son initiative à Salzbourg les 9-12 septembre 1968[8] et dont le thème portait sur les droits de l'homme et les moyens de communications de masse.

2. Presque deux ans plus tard, le 23 janvier 1970, et sur base de ces travaux, l'Assemblée adopta une Résolution portant Déclaration sur les moyens de communication de masse et les droits de l'homme[9] dans laquelle elle abordait aussi les mesures destinées à protéger l'individu contre les ingérences dans l'exercice de son droit au respect de la vie privée, étant exposé que « [l]e droit au respect de la vie privée consiste essentiellement à pouvoir mener sa vie comme on l'entend avec un minimum d'ingérence. Il concerne la vie privée, la vie familiale et la vie au foyer, l'intégrité physique et morale, l'honneur et la réputation, le fait de ne pas être présenté sous un faux jour, la non-divulgation de faits inutiles et embarrassants, la publication sans autorisation de photographies privées, la protection contre l'espionnage et les indiscrétions injustifiables ou inadmissibles, la protection contre l'utilisation abusive des communications privées, la protection contre la divulgation d'informations communiquées ou reçues confidentiellement par un particulier. Ne peuvent se prévaloir du droit à la protection de leur vie privée les personnes qui, par leurs propres agissements, ont encouragé les indiscrétions dont elles viendraient à se plaindre ultérieurement ».

En ce qui concerne les banques de données informatiques régionales, nationales ou internationales, la Déclaration soulignait le fait que l'individu ne devait pas être rendu totalement vulnérable par l'accumulation d'informations concernant sa vie privée[10]. En conséquence, ces banques de données ne devaient enregistrer que le minimum de renseignements nécessaires aux questions telles que les impôts, les systèmes de retraites, la Sécurité sociale, etc., ce qui évoque, aujourd'hui, le principe de la minimalisation des traitements de données.

---

[7] Voy. à ce sujet le rapport explicatif à la Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

[8] Les rapports présentés lors de cette Conférence sont disponibles via le service des Archives du Conseil de l'Europe.

[9] Résolution 428 (1970) portant Déclaration sur les moyens de communication de masse et les droits de l'homme, adoptée le 23 janvier 1970 par l'Assemblée consultative lors de sa 21e session ordinaire.

[10] Telle que celle-ci est définie dans la Résolution et reprise ci-dessus.

De manière générale et afin de lutter contre tous ces dangers qui menaçaient les individus, la Déclaration considérait que la législation nationale devait prévoir le droit d'intenter une action en justice contre les personnes qui se seraient rendues coupables d'atteintes de cette nature au droit au respect de la vie privée. À cet égard, elle a rappelé que le droit au respect de la vie privée protégeait l'individu « (…) non seulement contre l'ingérence des pouvoirs publics, mais aussi contre celle des particuliers et des institutions privées, y compris les moyens de communication de masse » et qu'en conséquence, la législation nationale devait comporter des dispositions garantissant cette (double) protection contre les autorités publiques et contre les autres particuliers.

3. À la suite de la Recommandation du 31 janvier 1968 relative aux droits de l'homme et aux réalisations scientifiques et technologiques modernes et du rapport du Comité d'experts en matière de droits de l'homme qui s'en était suivi, le Comité des Ministres en avait conclu que le problème de la protection de la vie privée vis-à-vis des banques de données électroniques était prioritaire. En 1971, il décida de créer un Comité sur la protection de la vie privée vis-à-vis des banques de données électroniques[11] et qui serait chargé d'étudier les aspects civils du droit à la vie privée affectée par les réalisations scientifiques et techniques modernes. Ce Comité a choisi de se pencher en premier sur les banques de données électroniques dans le secteur privé tout en envisageant l'élaboration d'un projet de Convention internationale à leur sujet[12]. À cet égard, lors des discussions de la 7e Conférence des Ministres européens de la Justice tenue à Bâle des 15 au 18 mai 1972[13] sur l'état d'avancement des travaux de ce Comité, il a été considéré que, s'il existait déjà des dispositions civiles et pénales pouvant être invoquées pour protéger la vie privée contre des abus liés à l'usage de registres informatiques traitant de données sensibles, il devait néanmoins être reconnu que la mise en œuvre de la technologie informatique avait créé de nouveaux problèmes en terme

[11] Le Comité sur la protection de la vie privée vis-à-vis des banques de données électroniques est un sous-comité du Comité européen de Coopération Juridique. Le Comité européen de coopération juridique est une instance intergouvernementale créée en 1963 sous les auspices du Comité des Ministres. Il est responsable des activités normatives du Conseil de l'Europe dans le domaine du droit public et privé. Il a pour rôle principal d'élaborer des normes communément admises par les États membres et de favoriser la coopération juridique entre eux. Le Comité européen de coopération juridique est constitué de représentants de tous les États membres – provenant principalement des ministères de la justice – et qui se réunissent une fois par an au siège du Conseil de l'Europe à Strasbourg.

[12] Ce qui aboutira le 28 janvier 1981 à l'adoption de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

[13] Conclusions de la 7e Conférence des Ministres européens de la Justice, Bâle, 15-18 mai 1972, Strasbourg, 5 juin 1972, CMJ/Conc. (72) 1.

de vie privée tant en ce qui concerne leur étendue que leur nature. Pour cette raison, il a semblé justifié de se concentrer sur les banques de données électroniques même si certains États membres souhaitaient aussi pouvoir réglementer les activités d'autres sortes de banques de données[14].

4. C'est dans ces circonstances que le Comité des Ministres adopta, le 26 septembre 1973, une Résolution relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé[15]. Dans celle-ci, le Conseil des Ministres a souligné le fait que les systèmes informatiques étaient utilisés à grande échelle et de manière constamment croissante dans le but d'enregistrer des données de caractère personnel. Il reconnaissait que, pour empêcher des abus lors de l'enregistrement, du traitement et de la diffusion d'informations de caractère personnel par les banques de données électroniques dans le secteur privé, il pouvait s'avérer nécessaire d'adopter des mesures législatives en vue de protéger les individus et qu'il était urgent, en attendant l'élaboration éventuelle d'un accord international, de prendre des mesures pour éviter de nouvelles divergences entre les droits des États membres en la matière.

L'objectif fondamental était donc, en quelque sorte, de s'assurer que les individus ne soient pas totalement à la merci des possibilités offertes par les technologies de l'information et de la communication[16], ce qui ressort encore mieux du rapport explicatif annexé à la Résolution du 26 septembre 1973. En effet, celui-ci explique que « (…) le développement de la science et de la technologie modernes permettant aux hommes d'atteindre un niveau de vie plus avancé, entraîne certains dangers menaçant les droits des individus ». C'est l'idée que le développement des nouvelles technologies génère des risques pour les individus.

Le rapport détaille quelque peu ces technologies et se réfère pour l'exemple à « (…) l'utilisation des nouvelles techniques appliquées à la surveillance ou à l'observation des personnes et pour l'enregistrement et le traitement des données les concernant ». Le double risque identifié ici est celui de l'espionnage de l'individu (c'est-à-dire la collecte d'informations à son insu), ainsi que celui de la compilation et de l'utilisation de

[14] Ce qui paraît pointer vers les fichiers de données (c'est-à-dire les données reprises sur un support en papier). Les conclusions de la 7e Conférence soulignent par ailleurs la différence qui peut exister entre les pays nordiques où le public dispose d'un accès libre aux documents officiers des autres pays où cet accès est moins libre.

[15] Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, adoptée par le Comité des Ministres le 26 septembre 1973 lors de la 224e réunion des Délégués.

[16] Sans préjudice de la volonté du Comité des Ministres de prévenir de nouvelles divergences dans la protection offerte en la matière par les États membres du Conseil de l'Europe.

ces informations. Le rapport rappelle que l'étude des législations nationales sur les droits de l'homme et les réalisations scientifiques et technologiques modernes effectuée par le Comité d'experts en matière de droits de l'homme du Conseil de l'Europe en 1968-1970 avait démontré que le droit existant n'offrait pas aux citoyens une protection suffisante contre les intrusions dans leur vie privée permises par les nouvelles technologies dès lors que les législations étudiées ne visaient, en général, que la protection du droit au respect de la vie privée sous un angle restreint tels que le secret de la correspondance et des télécommunications, l'inviolabilité du domicile etc.

Le rapport poursuit en exposant qu'il n'était pas acquis que la Convention européenne des droits de l'homme offrait des garanties satisfaisantes contre les intrusions dans la vie privée qui pouvaient être réalisées au moyen de nouvelles technologies puisque le Comité d'experts en matière de droits de l'homme avait relevé le fait que la Convention prenait plutôt en compte les ingérences dans l'exercice du droit au respect de la vie privée imputables aux autorités publiques plutôt que celles causées par des particuliers. À ce sujet, le rapport soulignait, à raison, que « la croissance rapide et la vulgarisation de la technologie des ordinateurs » avait créé une nouvelle source d'ingérence dans la vie privée des individus. Il attirait l'attention sur le fait que la quantité des services rendus possibles par les ordinateurs, tant dans les secteurs publics que privés, ne devait pas faire oublier que les objectifs poursuivis par le recours aux ordinateurs par rapport aux modes traditionnels de traitement de l'information n'avaient pas pour autant changé.

Toutefois, le rapport insistait sur la particularité des ordinateurs par rapport aux moyens antérieurs de traitement de l'information : « (…) l'extrême facilité avec laquelle les premiers ont simultanément surmonté tout un ensemble de problèmes posés par la gestion des informations : le grand volume des données, le système de leur stockage et de leur récupération, leur transfert à grande distance, leur interprétation correcte et, enfin, la rapidité avec laquelle ces opérations peuvent être effectuées ». Autrement dit, les ordinateurs sont autrement plus redoutables dans la gestion de l'information, ce qui les distingue radicalement des moyens utilisés auparavant. Le rapport note d'ailleurs que les ordinateurs permettent d'établir, « (…) sous la forme de « banques de données », des registres de données voire même des réseaux de registres de données reliés entre eux », et que ces « (…) « banques de données » sont susceptibles de fournir immédiatement et à grande distance un très grand nombre d'informations sur des individus ». Nous voyons resurgir, ici, l'appréhension du Comité des Ministres à l'égard des dangers liés à la compilation des informations relatives aux individus ainsi qu'à leur utilisation - risque accentué par la

possibilité de mettre les banques de données en réseau. Il y a là deux dangers qui sont distingués : la compilation d'informations relatives aux individus (que ce soit en silo, c'est-à-dire sur le même ordinateur ou serveur, ou en réseau, ce qui vise l'interconnexion entre les ordinateurs) d'une part, et, d'autre part, l'utilisation de ces informations, étant entendu que le Comité des Ministres estimait, à raison, que ces deux risques étaient rendus infiniment plus aigus par le recours à l'informatique (alors même qu'à cette époque les technologies de l'information et de la communication n'avaient pas atteint leur potentiel actuel).

D'un autre côté, le rapport indique que l'opinion publique avait manifesté son inquiétude en ce qui concerne « la possibilité d'une utilisation abusive de certaines informations personnelles à caractère confidentiel qui sont enregistrées électroniquement », tout en reconnaissant les avantages des traitements automatisés de données. Il notait que les moyens de défense des individus contre cet usage abusif étaient beaucoup plus réduits que ceux à leur disposition contre les fichiers traditionnels. Il notait encore que des informations inoffensives en elles-mêmes pouvaient être mises en corrélation et faire apparaître des aspects dont la révélation serait contraire aux intérêts des personnes concernées.

5. Rapidement après l'adoption de la Résolution du 26 septembre 1973 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé, le Comité des Ministres du Conseil de l'Europe a adopté, le 20 septembre 1974, une Résolution relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public[17]. Mais, si, dans la première Résolution du 26 septembre 1973, l'accent était plutôt mis sur la nécessité de protéger les individus conte les abus, ici, par contre, le Comité des Ministres se dit désireux de « (…) contribuer à la compréhension et à la confiance du public à l'égard des nouvelles techniques administratives que les autorités publiques mettent en œuvre dans les États membres en vue d'assurer une meilleure exécution des missions dont elles sont chargées » tout en reconnaissant la préoccupation du public en matière de protection de la vie privée des individus.

Nous pouvons voir là une sorte de modification de l'attitude du Comité des Ministres par rapport à l'approche qui semble prévaloir dans

[17] Résolution (74) 29 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur public, adoptée par le Comité des Ministres le 20 septembre 1974, lors de la 236e réunion des Délégués des Ministres. Il n'y a pas de rapport explicatif attaché à cette Résolution mais il est possible de considérer que le rapport explicatif de la Résolution (73) 22 a été écrit en ayant également en vue la rédaction de cette Résolution née des mêmes préoccupations et des mêmes travaux.

la Résolution précédente relatives aux banques de données électroniques dans le secteur privé. La présente approche n'est plus faite d'hostilité ou de méfiance mais plutôt de compréhension par rapport aux bénéfices qui peuvent en être retirés dans le secteur public. La différence entre les deux Résolutions pourrait aussi trouver une explication dans l'existence d'un préjugé défavorable envers les banques de données privées par rapport à l'aura positive dont bénéficieraient les autorités publiques en raison des missions d'intérêt public qui leur sont imparties. La dichotomie ne peut, en tout état de cause, pas être contestée ; la simple existence d'une Résolution distincte par secteur prouve la différence d'approche. Seules les causes de cette dichotomie sont ouvertes au débat.

6. Le Parlement européen n'était pas en reste et, dans la Résolution du 8 avril 1976[18], il avait chargé sa Commission juridique de faire rapport sur les actions communautaires à entreprendre ou à poursuivre en vue d'assurer la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique. La Commission juridique créa ensuite une sous-commission « Informatique et droits de la personne » qui organisa, au début de l'année 1978, un débat public sur l'informatique et les droits de la personne. Ses travaux débouchèrent sur l'adoption par le Parlement européen d'une Résolution en date du 5 juin 1979 sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique[19].

Dans cette dernière Résolution, le Parlement européen affirmait son souci de protéger les droits de la personne et soulignait sa sensibilité à la préoccupation de l'opinion publique devant « (…) les risques d'un usage erroné ou abusif des renseignements mémorisés dans les banques de données locales, régionales, nationales ou internationales », tout en rappelant le fait que le progrès technologique devait être mis au service de l'homme et qu'il était nécessaire de garantir la libre circulation de l'information au sein de la Communauté européenne et de réaliser « (…) un véritable marché commun de l'informatique (…) », tout en évitant que les législations nationales en matière de protection de la vie privée faussent la concurrence.

C'est dans ce contexte et en conséquence de ces objectifs et contraintes, que le Parlement européen appelait à la préparation d'une directive visant à harmoniser les législations des États membres en matière de protection des données « (…) à un niveau offrant le maximum de garanties aux citoyens de la Communauté » sur la base des Recommandations jointes

[18] *J.O.C.E.*, C 100 du 3 mai 1976, p. 27.
[19] *J.O.C.E.*, 5 juin 1979, C 140/34.

à la Résolution et qui contenaient les principes destinés à inspirer les normes communautaires en matière de protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique[20].

7. En parallèle, la poursuite et le développement des activités du Conseil de l'Europe en matière de protection des données ont abouti à l'adoption le 28 janvier 1981 de la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel[21] ainsi qu'à celle de nombreuses recommandations sectorielles et thématiques.

Le Rapport explicatif de la Convention 108 soulignait l'accroissement des risques auxquels étaient exposés les individus, ce qui justifiait un renforcement de leur protection. Le Rapport citait, entre autres, l'utilisation croissante de l'informatique à des fins administratives et de gestion, la capacité d'enregistrement des fichiers automatisés qui permettent aussi de procéder très rapidement à des opérations beaucoup plus variées. Le Rapport prévoyait aussi que « le traitement automatisé des informations continuera à s'imposer dans le domaine administratif et de gestion et cela notamment en raison de l'abaissement des coûts du traitement informatique des données, de l'apparition sur le marché de dispositifs de traitement « intelligents » et de la mise en place de nouveaux équipements de télécommunications pour la transmission des données ».

Il soulignait encore le fait que « Le « pouvoir de l'informatique » fait peser une responsabilité sociale correspondante sur les utilisateurs dans les secteurs privé et public. Dans la société moderne, une grande partie des décisions affectant les individus reposent sur des données enregistrées dans des fichiers informatisés : feuilles de paie, dossiers de sécurité sociale, dossiers médicaux, etc. Il est essentiel que les responsables de ces fichiers s'assurent que les avantages indéniables qu'ils peuvent obtenir du traitement automatisé des données n'aboutissent, en même temps, à affaiblir la position des personnes concernées par les données enregistrées. Pour cette raison ils devraient veiller à la bonne qualité des informations qui leur

[20] L'O.C.D.E. était plus préoccupé par la libre circulation des données. Voy. la Recommandation du Conseil de l'Organisation de coopération et de développement économiques concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel, adoptée le 23 septembre 1980.

[21] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du Conseil de l'Europe, 28 janvier 1981, Série des traités européens, n° 108. Cette Convention est souvent dénommée « Convention 108 ». À ce jour, cinquante pays ont adhéré à cette Convention, ce qui amène son audience à plus de huit cent millions d'individus.

sont confiées, s'abstenir d'enregistrer des informations qui ne sont pas nécessaires à la poursuite de la finalité déclarée, se garder de diffuser des informations sans autorisation ou d'en abuser, et protéger les données, le matériel et le logiciel, de tout risque d'endommagement ».

En matière de flux transfrontières, le Rapport attirait l'attention sur le fait que « [e]n pratique toutefois la protection des personnes perd en efficacité lorsque l'aire géographique s'élargit. On craint notamment que les utilisateurs ne soient tentés d'éviter les contrôles imposés par la protection des données en déplaçant leurs opérations, en totalité ou en partie, vers des « paradis de données », c'est-à-dire dans des pays ayant des lois sur la protection des données moins strictes, voire sans lois ».

8. De son côté, la Communauté européenne [devenue Union européenne] s'était attelée à finaliser la difficile tâche qui consistait à mettre en place un cadre juridique commun à tous ses États membres en matière de traitements des données à caractère personnel. Cette action se traduira, dans un premier temps, par l'adoption de la 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[22].

L'objectif matériel poursuivi par la directive 95/46/CE était de garantir les droits et libertés de l'individu en matière de traitements de données. L'analyse des considérants de la directive permet de mieux préciser cet objectif. D'abord, la directive rappelait les objectifs généraux propres à l'Union européenne : la réalisation d'une union toujours plus étroite entre les États membres, assurer par une action commune le progrès économique et social en éliminant les barrières qui divisent l'Europe, préserver et conforter la paix et la liberté, et promouvoir la démocratie en se fondant sur les droits fondamentaux reconnus aux individus. Ensuite, la directive se concentrait sur les systèmes de traitements de données en rappelant qu'ils étaient au service de l'homme et qu'ils devaient respecter les libertés et droits fondamentaux des individus et notamment la vie privée, tout en contribuant au progrès économique et social, au développement des échanges et au bien-être de la population. La directive rappelait encore que l'établissement et le fonctionnement du marché intérieur nécessitaient la libre circulation des données et la sauvegarde des droits fondamentaux des individus. Par ailleurs, elle soulignait le développement des

[22] *J.O.C.E.*, L 281, 23 novembre 1995, p. 31. Le développement de la protection des données au sein de l'Union européenne se poursuivra par la reconnaissance de l'existence d'un droit fondamental à la protection des données inscrit dans la Charte des droits fondamentaux et par l'adoption d'instruments à vocation plus sectorielle ou thématique.

traitements de données dans les divers domaines de l'activité économique et sociale, soutenu en cela par les progrès des technologies de l'information et de la communication. Elle attirait l'attention sur le fait que l'intégration économique et sociale (qui va de pair avec l'établissement et le fonctionnement du marché intérieur) entraînerait une augmentation des flux de données entre les acteurs des activités économiques et sociales des États membres, tant dans le secteur privé que public. Elle soulignait aussi le fait que le renforcement de la coopération scientifique et technique, ainsi que la mise en place coordonnée de nouveau réseaux de télécommunications dans l'Union européenne, nécessiteraient et faciliteraient les flux de données entre les États membres. Enfin, la directive ajoutait que les différences en matière de protection des données dans les États membres pouvaient empêcher les flux de données entre eux et par-là, faire obstacle à l'exercice d'activités économiques au niveau de l'Union européenne, fausser la concurrence et empêcher des administrations publiques de remplir leurs obligations communautaires.

Il ressort de ces considérations que l'objectif matériel poursuivi par la directive 95/46/CE consistait à protéger les droits et libertés des individus en matière de traitements de données dans le cadre de l'établissement et du fonctionnement du marché intérieur, sans que cela ne puisse aboutir à un affaiblissement des protections existantes. Au contraire, la directive devait mener à garantir un niveau de protection élevé dans l'Union européenne[23]. Ce faisant, la directive inscrivait l'action de l'Union européenne en matière de protection des données dans la sphère des compétences qui sont les siennes. Elle constatait le développement des traitements de données au sein des États membres ainsi que celui des transferts de données entre les États membres et elle soulignait le fait que ces traitements de données devaient respecter les droits et libertés des individus sans que cela ne contrevienne aux règles qui gouvernent l'établissement et le fonctionnement du marché intérieur.

9. Après avoir procédé au rapprochement des législations des États membres en matière de traitement de données par l'adoption de la directive 95/46/CE, l'Union européenne a poursuivi le développement du cadre juridique de la protection des données. Principalement, elle a élevé le droit à la protection des données au titre de droit fondamental[24], adopté

[23] Considérant n° 10 de la directive 95/46/CE.

[24] Adoptée à Nice le 7 décembre 2000, la Charte des droits fondamentaux de l'Union européenne proclame le droit à la protection des données (*J.O.C.E.*, 18 décembre 2000, C 364/01, art. 8) :

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

un Règlement propre aux institutions européennes[25] ainsi qu'une directive relative à la protection de la vie privée dans le secteur des communications électroniques[26]. Dans le même temps, des experts se sont penchés (relativement rapidement) sur la nécessité de réformer le cadre juridique général établi par la directive 95/46/CE – les uns prétextant des évolutions technologiques fulgurantes, les autres des problèmes dans la mise en œuvre du régime juridique général établi par la directive 95/46/CE[27].

---

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.
3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Ce droit est rappelé dans l'article 16 du Traité sur le fonctionnement de l'Union européenne qui énonce ce qui suit à propos de la protection des données à caractère personnel au titre de ses dispositions d'application générale :

1. Toute personne a droit à la protection des données à caractère personnel la concernant.
2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne.

[25] Règl. (CE) 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.

[26] Il s'agit de la directive 2002/508/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Il faut y ajouter le Règl. (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

Elle avait aussi adopté une directive 2006/24/CE en date du 15 mars 2003 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, mais cette directive fut annulée par la Cour de Justice de l'Union européenne (voy. l'arrêt du 8 avril 2014 de la Cour de justice de l'Union européenne dans les affaires jointes C-293/12 et C-594/12).

[27] Voy. déjà : le Premier rapport de la Commission sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) (COM(2003) 265 final, du 15 mai 2003 ; l'étude « Analysis and impact study on the implementation of Directive 95/46/CE in Member States » ; la communication de la Commission au Parlement européen et au Conseil consacrée au "Suivi du Programme de travail pour une meilleure mise en application de la directive sur la protection des données" (COM(2007) 87 final, du 7 mars 2007); ainsi que la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions intitulée « Une approche globale de la protection des données à

Après quelques hésitations sur le bien-fondé de la démarche et puis d'intenses activités d'influence en tout genre, le cadre juridique général de la protection des données a finalement été réformé par l'adoption du Règlement général sur la protection des données du 27 avril 2016[28] dont les règles sont d'application depuis le 25 mai 2018. Cette réforme modifie en profondeur l'architecture du cadre juridique existant et démultiplie les dispositions applicables[29].

Ce Règlement expose, longuement et de manière relativement incohérente, paradoxale et contradictoire, dans une certaine mesure, les raisons de son adoption. Il invoque pêle-mêle le droit à la protection des données, la nécessité que les principes et règles de la protection des personnes à l'égard du traitement des données qui les concernent doivent respecter les droits et libertés des individus, peu importe leur nationalité ou résidence[30],

caractère personnel dans l'Union européenne » (COM(2010) 609 final, du 4 novembre 2010). Voy. aussi le considérant n° 9 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119, 4 mai 2016, p. 1. Voy. enfin, H. Burkert, *Privacy – Data Protection. A German/European Perspective*, Second Symposium of the German American Academic Council's Project « Global Networks and Local Values », Woods Hole, Massachussetts, 1999.

[28] Le Règlement a été adopté en même temps (et à titre de condition préalable) **d'une part** que la directive 2016/680/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, **et, d'autre part**, que la directive 2016/681/UE du Parlement européen et du Conseil du 27 avril 2016 relative à la l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. Le Règlement s'applique dans vingt-huit pays et concerne plus de cinq cent millions d'individus.

[29] Ce qui est de nature à permettre aux détracteurs de la protection des données de dénoncer son caractère impraticable.

[30] Le sens de cette partie du Considérant n° 2 n'est pas clair. Il est acquis depuis longtemps que la protection des droits et libertés profite à toute personne qui se trouve sur le territoire d'un État, indépendamment de sa nationalité (c'est l'application immédiate des dispositions en matière de droits fondamentaux). Il demeure alors la référence de l'application de la protection indépendamment de la résidence de la personne, ce qui laisse perplexe. Soit cela n'a pas de sens, soit le Règlement veut simplement dire que la protection doit être la même quel que soit l'État membre sur le territoire duquel se trouve la personne et ce, dans le cadre d'une vision très avancée de l'intégration européenne où il ne subsisterait que le territoire de l'Union européenne, d'une part et, d'autre part, que le Règlement protège aussi les personnes qui ne se trouvent pas sur le territoire de l'Union européenne mais dont les données qui les concernent sont traitées par un responsable de traitement qui serait soumis au Règlement.

tout en soulignant le caractère relatif et fonctionnel[31] du droit à la protection des données, la contribution de la protection des données aux objectifs poursuivis par l'Union européenne[32], l'apport des traitements de données à l'humanité[33], l'intégration économique et sociale résultant du fonctionnement du marché intérieur et de l'augmentation corrélative des flux transfrontaliers de données[34], le développement des technologies de l'information et de la communication[35] et le besoin de susciter la confiance pour assurer le développement de l'économie numérique[36].

Heureusement, les dispositions du Règlement sont plus claires dans la détermination des deux objectifs qu'il poursuit[37]. D'une part, le Règlement vise à protéger les droits et libertés des personnes physiques à l'égard du traitement de données à caractère personnel et en particulier leur droit à la protection des données à caractère personnel dans le cadre de la réalisation des objectifs de l'Union européenne. D'autre part, le Règlement orga-

[31] Toute la question est de savoir ce qu'il faut entendre, ici, par droit « fonctionnel ». À ce sujet, voy. S. PLATON, « Le périmètre de l'obligation de respecter les droits fondamentaux en droit de l'Union européenne », in T. TINIERE et C. VIAL (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, coll. Droit de l'Union européenne, Bruxelles, Bruylant, 2015. Le recours à ce qualificatif peut être l'expression d'un recul en matière de développement du système de protection des droits fondamentaux de l'Union européenne.

[32] Le considérant n° 2 se réfère à cet égard à « la création d'un espace de libertés, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques ». Toute la question est de savoir si formuler ce genre de lieu commun présente un quelconque intérêt.

[33] Le considérant n° 4 expose plus précisément que « [l]e traitement des données à caractère personnel devrait être conçu pour servir l'humanité ». Dans sa généralité, cette formule est excessive, sinon outrancière. En quoi l'exploitation de données par une entreprise internationale étrangère à l'Union européenne à des fins purement lucratives pourrait-elle servir l'humanité ? Formulée de manière plus raisonnable, cette formule pourrait exprimer l'espoir que certains traitements de données soient de nature à faire avancer la science, par exemple, mais, dans ce cas, il conviendrait de l'exprimer de manière plus appropriée notamment pour expliquer les conditions de licéité particulières qui régiraient les traitements de données à des fins scientifiques.

[34] Voy. le considérant n° 5. Il est amusant de constater la facilité avec laquelle le Règlement, comme la directive 95/46/CE auparavant, considère comme étant acquis et légitime le besoin de centraliser les données en intra-européen ou de les transférer d'un État membre à l'autre alors qu'en réalité, la première chose qu'il faudrait faire, c'est se pencher sur la justification de ces flux de données en intra-européen par rapport aux droits et libertés des individus. C'est au moment de procéder à la balance des intérêts en présence dans ce genre de situations que se révèle au grand jour la réalité de la protection des données au sein de l'Union européenne.

[35] Voy. le considérant n° 6.

[36] Voy. le considérant n° 7.

[37] Voy. art. 1er du Règlement.

nise la libre circulation de ces données au sein de l'Union européenne : celle-ci ne peut être ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

10. Dans le même temps, le Conseil de l'Europe s'était aussi attelé à la modernisation de la Convention 108, ce qui s'est concrétisé par l'adoption en date du 18 mai 2018 d'un Protocole d'amendement qui a donné lieu à un texte consolidé connu sous le nom de Convention modernisée pour la protection des personnes à l'égard du traitement des données à caractère personnel ou, en abrégé, la **Convention 108 +**[38]. Un des risques mis en avant dans le Rapport explicatif du Protocole est que « [l]a dignité humaine requiert la mise en place de garanties lors du traitement de données à caractère personnel, afin que les individus ne soient pas traités comme de simples objets ». Car c'est bien là un des enjeux majeurs de la protection des données aujourd'hui : le risque de réification des individus[39]. Dans la société de l'information, cela vise le risque de voir l'individu n'être plus qu'un objet et non plus un sujet de droit ou, plus simplement, de passer du statut de personne à celui d'être exploité ou à tout le moins exploitable.

11. On voit, au travers de ces quelques éléments choisis, que la protection des données s'entend d'une protection des individus contre les risques auxquels les exposent les traitements de données à caractère personnel qui les concernent. Autrement dit, les individus sont vulnérables face aux technologies de l'information et de la communication en raison des risques auxquels les exposent les traitements de données à caractère personnel. Il demeure maintenant à voir comment ces risques sont pris en considération et comment il est tenté de les maîtriser. Cela est d'autant plus nécessaire aujourd'hui que ces risques culminent avec le développement du *cloud computing* (le recours à des ressources extérieures), du *big data* (la collecte et la conservation de quantités prodigieuses de données, de *data mining* (l'exploitation de ces quantités phénoménales de données) et *d'Internet des choses* (IoT) (la mise en place de réseaux de capteurs qui collectent également énormément de données), aidés en cela par des

[38] Il s'agit du texte consolidé de la Convention 108 tel que modifié par le Protocole du 18 mai 2018 d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) (CM(2018)2-final, STE n 223. Voy. aussi son rapport explicatif).

[39] Sur la notion de réification, voy. déjà : L. ROBERT, « Réification et marchandisation du corps humain dans la jurisprudence de la Cour EDH. Retour critique sur quelques idées reçues », *La Revue des Droits de l'Homme*, 2015/8.

infrastructures et des équipements de télécommunication toujours plus performants.

SECTION 2. – La protection des données : un cadre juridique pour les traitements de données à caractère personnel

12. Comme nous l'avons esquissé ci-dessus, la protection des individus en matière de traitements de données à caractère personnel est poursuivie en Europe par la mise en place d'un cadre juridique spécifique établi par le Règlement général sur la protection des données (le Règlement). Ce dernier fixe les conditions à respecter pour traiter ces données et reconnaît des droits à la personne à l'égard des données qui la concernent et qui font l'objet d'un traitement, tout en mettant en place des organes, des procédures et des sanctions spécifiques afin d'assurer l'effectivité de ce nouveau cadre juridique, étant entendu que le droit à la protection des données a été consacré au titre de droit fondamental des individus au niveau de l'Union européenne.

§ 1. Les principes relatifs aux traitements de données à caractère personnel

13. Les sept principes auxquels doivent se conformer les traitements de données sont bien connus :

1) Les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (ce sont les principes de licéité, de loyauté et de transparence) ;

2) Les données doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités (c'est le principe de la limitation des finalités)[40] (le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas incompatible n'est pas incompatible avec les finalités initiales pour autant qu'il soit soumis à des garanties appropriées pour les

[40] Voy. Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, WP 203 2 April 2013.

droits et libertés de la personne concernée. Ces garanties doivent garantir la mise en place de mesures techniques et organisationnelles singulièrement pour garantir le respect du principe de la minimisation des données[41]. Dans la mesure du possible, le traitement ultérieur ne devrait pas ou plus permettre l'identification de la personne concernée) ;

3) Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (c'est le principe de minimisation des données). La réaffirmation, bienvenue, de ce principe est, cependant, paradoxale au regard des orientations prises actuellement en matière de traitement de l'information et notamment du phénomène du Big Data qui ne mise plus sur la qualité intrinsèque d'une l'information mais plutôt sur l'application de techniques statistiques destinées à donner de la valeur informationnelle à des masses d'information qui, prises séparément, en sont largement dépourvues dans la plupart des cas ;

4) Les données doivent être exactes et, si nécessaire, tenus à jour et toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (c'est le principe d'exactitude) ;

5) Les données ne peuvent être conservées sous une forme qui permette l'identification des personnes concernées pour une durée qui excéderait ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Les données peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques pour autant que leur traitement soit soumis à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties doivent garantir la mise en place de mesures techniques et organisationnelles singulièrement pour garantir le respect du principe de la minimisation des données[42]. Il faut recourir à

[41] Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière. La pseudonymisation est le traitement de données à caractère personnel réalisé de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable (art. 4.5) du Règlement).

[42] Ces mesures peuvent comprendre la pseudonymisation, dans la mesure où ces finalités peuvent être atteintes de cette manière.

des traitements ultérieurs qui ne permettent pas ou plus d'identifier les personnes concernées chaque fois que cela se révèle possible ;

6) Les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (c'est le principe d'intégrité et de confidentialité) ;

7) Le responsable du traitement est responsable du respect de ces principes. En outre, et c'est nouveau dans la forme, il doit être en mesure de démontrer que ces principes sont effectivement respectés (c'est le principe de responsabilité)[43].

§ 2. Les principes relatifs à la licéité des traitements de données à caractère personnel

14. Ensuite, le Règlement énumère les catégories d'hypothèses dans lesquelles il est, *a priori*, licite (c'est-à-dire conforme à ce qu'autorise le droit), de traiter des données à caractère personnel. Il n'est donc permis de traiter des données que dans une des hypothèses suivantes[44] :

1) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

2) 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 ;

3) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

4) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

5) 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 ;

---

[43] Voy. Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, WP 173 13 July 2010.

[44] Voy. art. 6.1 du Règlement. L'article 6.2 prévoit la possibilité de régimes particuliers pour les traitements imposés par la loi ou réalisés dans l'intérêt public ou dans l'exercice de l'autorité publique dans le chef du responsable du traitement. Voy. art. 6.4 à propos des traitements ultérieurs.

6) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel (notamment lorsque la personne concernée est un enfant). Cette hypothèse ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

15. Il est présumé, pour chacune de ces catégories, qu'il est légitime, en général, de traiter des données. Pour le dire autrement, chacune de ces catégories est censée représenter une situation dans lesquelles les intérêts en présence sont dans un équilibre acceptable. Ces intérêts à prendre en considération sont ceux du responsable du traitement, de la personne concernée et de la collectivité. Dans la droite ligne des mécanismes de légitimation mis en place dans la directive 95/46/CE, il faut, bien entendu, vérifier dans chaque cas d'espèce pour chaque traitement pris et considéré séparément et individuellement, si cet équilibre entre les trois axes d'intérêts est bien respecté *in concreto* et non seulement *a priori* et *in abstracto*. À cet égard, la modification dans le temps de l'équilibre des intérêts en présence aura pour effet d'ôter la légitimité du traitement de données pour le futur ; il faudra donc y mettre fin sauf à trouver une solution pour rééquilibrer de manière satisfaisante les intérêts en présence. Il faut répéter que l'appréciation de la légitimité d'un traitement de données est sensible aux autres aspects de la mise en œuvre de la protection des données, comme le niveau de confidentialité et de sécurité du traitement de données, le niveau de mise en œuvre des droits de la personne concernée, le niveau de contrôle assuré par l'autorité national de contrôle, le degré de nécessité de la finalité poursuivie, la manière d'assurer les droits de la personne concernée, etc.

§ 3. Les principes relatifs au consentement de la personne concernée au traitement de données à caractère personnel qui la concernent

16. Ainsi que nous l'avons vu, le consentement de la personne concernée, à l'instar de toutes les autres hypothèses de légitimation, induit une présomption de licéité du traitement de données qui la concernent – une présomption d'équilibre entre les intérêts en présence. Le responsable du traitement doit être en mesure de prouver que la personne a bien donné

son consentement[45], ce qui signifie que le responsable du traitement ne peut pas se contenter d'imposer à la personne concernée de prouver qu'elle n'aurait pas consenti au traitement de données. Il doit démontrer lui-même que la personne concernée a bien consenti étant entendu que celle-ci peut toujours combattre les prétentions du responsable du traitement. Il doit aussi prouver avoir informé la personne concernée de son droit à retirer son consentement.

Il arrive fréquemment que la demande de consentement soit noyée dans un mélange d'autres requêtes ou dispositions. Dans ce cas, si le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande doit être présentée sous une forme qui la distingue clairement des autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. La partie de cette déclaration qui méconnait ces règles n'est pas contraignante[46], ce qui signifie, concrètement, que la personne concernée peut renoncer à s'en plaindre et ratifier l'illégalité en cause.

La personne concernée peut toujours retirer son consentement à tout moment[47] et sans avoir à se justifier – même si le Règlement ne rappelle cette dernière règle. Le retrait du consentement n'invalide pas les opérations antérieures[48]. Par contre, elles empêchent la poursuite du traitement de données. La personne concernée doit avoir été informée du droit de retirer son consentement avant de le donner[49]. Comme l'énonce le Règlement, il doit être aussi simple de retirer que de donner son consentement[50].

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat[51].

17. Nonobstant les commentaires qui lui ont été adressés à ce sujet lors de la consultation publique de son document revisité contenant des lignes directrices en matière de consentement sous le Règlement, le Comité européen de protection des données a maintenu l'affirmation selon laquelle un responsable de traitement devait choisir une (et une seule) base de

[45] Art. 7.1 du Règlement.
[46] Art. 7.2 du Règlement.
[47] Art. 7.3 du Règlement.
[48] Art. 7.3 du Règlement.
[49] Art. 7.3 du Règlement.
[50] Art. 7.3 du Règlement.
[51] Art. 7.4 du Règlement.

licéité pour fonder le traitement de données parmi les six choix offerts par l'article 6 du Règlement et que s'il avait choisi le consentement pour tout ou partie du traitement de données, il devait mettre fin au traitement de données si la personne concernée retirait son consentement ou si le consentement se révélait invalide[52]. Cette affirmation est inexacte et explicitement contredite par le Règlement lui-même. En effet, l'article 6.1 du Règlement énonce déjà que « [l]e traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est rempli (…) », ce qui prouve déjà à suffisance que plusieurs bases de licéité peuvent fonder un traitement de données. De plus, l'article 17 du Règlement expose, à propos du droit à l'effacement (« droit à l'oubli »), que le responsable du traitement doit effacer les données dans les meilleurs délais lorsque la personne concernée a retiré son consentement sur lequel était fondé le traitement (que ce soit sur pied de l'article 6.1.a) ou 9.2.a)) et lorsqu'il n'existe pas d'autre fondement juridique au traitement. Ceci démontre de manière incontestable qu'un même traitement peut reposer sur plusieurs bases juridiques différentes.

Autrement dit, contrairement à l'opinion du Comité européen de protection des données, le responsable du traitement peut et, dans certains cas, doit renforcer la licéité de son traitement de données en ajoutant le consentement de la personne concernée (comme en matière de recherche scientifique)[53].

18. Sur le fond, il est difficile de se défaire de l'idée que, si les contraintes mises par le Comité en matière de consentement sont idéales, il n'en demeure pas moins qu'elles ne correspondent en rien à la réalité ni à quoi que ce soit qui soit praticable dans beaucoup d'hypothèses. Toute la question est donc de savoir s'il n'aurait pas mieux fallu agir sur d'autres points de la règlementation pour contrebalancer des faiblesses dans la légitimation des traitements de données lorsqu'elle est fondée sur le consentement de la personne concernée. Ainsi, par exemple, on pourrait augmenter le bénéfice que la personne concernée serait susceptible d'en retirer comme des retours sur son état de santé, par l'accès aux traitements médicaux disponibles découverts suite à la recherche scientifique, par un droit d'accès plus dynamique (par exemple, une information structurée à intervalles réguliers transmise d'initiative du responsable du traitement

[52] Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices sur le consentement sous le Règlement 2016/679*, adopté le 28 novembre 2017 et revu et adopté en dernier le 10 avril 2018, WP 259 rev.01, p. 23, pt 6.

[53] À ce sujet, voy. : J. Herveg et J.-M. Van Gyseghem, « L'impact du Règlement général sur la protection des données dans le secteur de la santé », in *Le Règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018 (à paraître), p. 730, n° 39.

vers la personne concernée) ou par la mise en place d'une réelle gouvernance de la société de l'information avec de véritables organes démocratiques et judiciaires dédicacés à la régulation des activités humaines dans ce nouveau monde virtuel.

19. Enfin, la question du sort à donner au consentement obtenu sous l'empire de la directive 95/46/CE est incertain. Le considérant n° 171 énonce à ce sujet que « [l]es traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées ». Le Comité ne dit pas autre chose : le consentement est toujours valable à condition d'être conforme aux conditions posées par le Règlement. Autrement dit, il n'est pas possible de soutenir que les consentements obtenus sous le couvert de la directive 95/46/CE seront tous considérés comme demeurant valides au-delà du 25 mai 2018. Pour être plus précis, ce n'est pas que le consentement obtenu antérieurement ne serait plus valide ; en réalité, il ne peut plus produire d'effet juridique s'il n'est pas conforme aux nouvelles règles. Cette solution est conforme aux règles usuelles en matière d'application des lois dans le temps : en règle, la validité d'un acte s'apprécie au jour de la formation de celui-ci. En conséquence, la validité des actes passés avant le 25 mai 2018 devrait s'apprécier au regard de la législation applicable adoptée en transposition de la directive 95/46/CE, au jour de la formation de cet acte. Par contre, l'adoption d'une nouvelle règlementation peut modifier les effets juridiques à produire par cet acte à partir de l'entrée en vigueur de celle-ci.

§ 4. Les principes relatifs au consentement des enfants mineurs d'âge en ce qui concerne les services de la société de l'information

20. Dans une approche traditionnelle, les enfants mineurs représentent une catégorie classique de personnes vulnérables. En règle, la

représentation d'un enfant mineur d'âge en matière personnelle est encadrée par la Convention de New-York du 26 janvier 1990 relative aux droits de l'enfants[54] et puis par le droit de chaque État membre en matière de capacité d'exercice des enfants mineurs d'âge. La règle généralement admise est que l'infans est représenté par ses parents, que l'enfant jusqu'à 15-16 ans est assisté par ses parents dans les décisions personnelles et, qu'à partir de cet âge, il prend seul les décisions importantes en matière personnelle, étant entendu qu'un certain nombre de décisions très personnelles ne sont susceptible d'aucune représentation, quel que soit l'âge de l'enfant (comme le mariage, la vie amoureuse ou sexuelle et le choix de ses relations personnelles – les amis, par exemple).

En matière de traitements de données à caractère personnel, le Règlement prévoit qu'un enfant doit être âgé d'au moins seize ans pour pouvoir consentir au traitement de données dans le cadre d'une offre de services de la société de l'informations qui lui est directement adressée, et que, s'il est âgé de moins de seize ans, le traitement n'est licite que si le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant[55]. Comme le lui permettait le Règlement, le législateur fédéral belge a choisi d'abaisser cet âge à treize ans[56].

En ce qui le concerne, le responsable du traitement doit simplement s'efforcer raisonnablement de vérifier, en pareil cas, que le consentement a été donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles[57]. Le Règlement précise que cette règle ne modifie pas le droit général des contrats des États membres[58], ce qui signifie que si le consentement n'est pas valable mais que le responsable du traitement s'est raisonnablement efforcé de vérifier que le consentement avait été donné ou autorité par le titulaire de la responsabilité parentale à l'égard de l'enfant, le responsable du traitement ne pourra pas se voir reprocher une violation du Règlement sur ce point mais le contrat risque de ne pas en être plus valable pour autant.

21. Le Règlement ne règle pas la question du sort à réserver au consentement donné par des parents au nom et pour compte de leur enfant mineur

[54] Voy. déjà les articles 12 (droit d'exprimer librement son opinion sur toute question l'intéressant) 13 (liberté d'expression) ou 16 (droit au respect de la vie privée).

[55] Art. 8.1 du Règlement. Les États membres peuvent prévoir de descendre l'âge jusqu'à treize ans.

[56] Voy. art. 7 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

[57] Art. 8.2 du Règlement.

[58] Art. 8.3 du Règlement.

d'âge lorsque ce dernier devient majeur. Le consentement demeure-t-il valide ou faut-il rechercher le consentement de l'enfant devenu majeur ? En matière de recherche clinique, la règle veut qu'il faille rechercher le consentement de ce dernier ou, à tout le moins, lui donner la possibilité de s'opposer à la poursuite de l'essai. Il n'existe aucune raison de ne pas appliquer, *mutatis mutandis*, la même règle en matière de traitement de données. Le consentement ainsi donné par les parents devrait cesser de produire ses effets au jour de la majorité de l'enfant. La règle est impitoyable mais elle est la conséquence logique de l'approche irréaliste adoptée par le Comité (et quelque part par le Règlement et la directive 95/46/CE auparavant) d'un consentement idéalisé qui n'existe pas dans le monde réel.

§ 5. Les principes relatifs aux traitements portant sur des catégories particulières de données à caractère personnel

22. La règle est bien connue et n'a pas changé : le traitement portant sur des catégories particulières de données à caractère personnel (données sensibles ci-après tel que la directive 95/46 les nommait) est interdit. Plus précisément, le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, sont interdits[59]. Cette interdiction ne s'applique pas dans les hypothèses suivantes[60], sans préjudice de la nécessité de vérifier *in concreto* l'existence d'un juste équilibre entre les intérêts en présence pour chaque traitement :

1) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction ne peut pas être levée par la personne concernée ;

2) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et

[59] Art. 9.1 du Règlement.

[60] Art. 9.2 du Règlement. Toutefois, les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé (art. 9.4 du Règlement).

de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée ;

3) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

4) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées ;

5) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;

6) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;

7) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un 'État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

8) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées à l'article 9.3 du Règlement[61] ;

[61] Ces données doivent être traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité,

9) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

10) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89.1 du Règlement, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Les États membres peuvent toutefois adopter des règles matérielles particulières en matière de traitements de données génétiques, de données biométriques ou de données relatives à la santé, dans la limite de ce que permet la jurisprudence de la Cour européenne des droits de l'homme en matière de protection des données et la Convention 108 [+].

§ 6. Les principes relatifs aux traitements de données relatives aux condamnations pénales et aux infractions

23. Le traitement des données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes, fondé sur l'article 6.1 du Règlement, ne peut être effectué que sous le contrôle de l'autorité publique ou que si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique[62].

---

ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents.

[62] Art. 10 du Règlement.

§ 7. Les principes relatifs aux traitements de données qui ne nécessitent pas l'identification de la personne concernée

24. Si les finalités pour lesquelles des données sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le Règlement[63]. Le Règlement prévoit que, lorsque le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareil cas, la personne concernée doit fournir des informations complémentaires qui permettent de l'identifier aux fins d'exercer son droit d'accès, son droit de rectification, son droit à l'effacement, son droit à la limitation du traitement, son droit à la notification de la rectification ou de l'effacement de données ou de la limitation du traitement, ou encore son droit à la portabilité des données[64]. Tout ceci n'empêche pas que le responsable du traitement soit, pour le surplus, soumis à l'ensemble des obligations qui découlent du Règlement et qui s'imposent à lui.

§ 8. Les obligations générales à charge du responsable de traitement et du sous-traitant

25. Ensuite, la protection des données se réalise par l'imposition de toute une série de contraintes à charge des personnes qui traitent des données à caractère personnel. Outre le respect des principes applicables au traitement de données, le responsable du traitement et son sous-traitant éventuel doivent se soumettre à toute une série d'obligations générales qui représentent autant de nouvelles règles matérielles uniformes à respecter.

A) Le principe de la responsabilité du responsable du traitement

26. La première obligation générale du responsable du traitement est de s'assurer que les traitements de données sont effectués conformément aux règles fixées par le Règlement et il doit être en mesure de le démontrer. À cet effet, il doit mettre en œuvre des mesures techniques et organisationnelles appropriées, en tenant compte de la nature, de la portée,

[63] Art. 11.1 du Règlement.
[64] Voy. art. 11.2 du Règlement.

du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité peut varier, pour les droits et libertés des personnes physiques. Le responsable du traitement doit aussi mettre en œuvre des politiques appropriées en matière de protection des données qui sont proportionnées au regard des activités de traitement. Il doit réexaminer toutes ces mesures et les actualiser si nécessaire[65], le tout sur une base régulière ainsi qu'ensuite d'incidents.

B) La protection des données dès la conception

27. La seconde obligation générale du responsable du traitement est de mettre en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées[66] destinées à mettre en œuvre les principes relatifs à la protection des données[67] de façon effective, et qui sont destinées à assortir le traitement des garanties nécessaires pour répondre aux exigences fixées par le Règlement et protéger les droits de la personne concernée. Ces mesures doivent tenir compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité peut varier) que le traitement présente pour les droits et libertés des personnes physiques, et qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée[68].

C) La protection des données par défaut

28. La troisième obligation générale du responsable du traitement est de mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient traitées. Cela s'applique tant à la quantité de données

[65] Voy. art. 24 du Règlement. L'application d'un code de conduite approuvé ou de mécanismes de certification approuvés peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement.

[66] Comme la pseudonymisation.

[67] Comme la minimisation des données.

[68] Sur tout ceci, voy. art. 25.1 du Règlement. Un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de ces exigences.

à caractère personnel collectées, qu'à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures doivent garantir que, par défaut, les données à caractère personnel ne soient pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée[69].

D) Les responsables conjoints du traitement de données

29. La possibilité d'avoir des responsables conjoints du traitement[70] n'est pas neuve mais le Règlement précise qu'ils doivent définir de manière transparente leurs obligations respectives pour garantir le respect des règles en matière de protection des données, notamment en ce qui concerne l'exercice des droits de la personne concernée, ainsi que leurs obligations respectives quant à la communication des informations à fournir à la personne concernée. Ils peuvent notamment désigner un point de contact pour les personnes concernées. Cette répartition des obligations doit se faire par la voie d'un accord entre eux sauf si, et dans la mesure, où leurs obligations respectives sont définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis[71]. Cet accord doit refléter fidèlement les rôles respectifs des responsables conjoints du traitement ainsi que leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord doivent être mises à la disposition de la personne concernée[72]. En tout état de cause, la personne concernée peut exercer les droits qui lui sont reconnus en matière de protection des données à l'égard de et contre chacun des responsables du traitement[73].

[69] Voy. art. 25.2 du Règlement. De nouveau, un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect de ces exigences.

[70] Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

[71] Voy. art. 26.1 du Règlement.

[72] La loyauté impose, en réalité, que cette information soit communiquée volontairement par les responsables du traitement lors de l'information due aux personnes concernées.

[73] Voy. art. 26.3 du Règlement.

E) Les représentants des responsables du traitement ou des sous-traitants qui ne sont pas établis dans l'Union européenne

30. Lorsque le Règlement s'applique à un responsable du traitement ou à un sous-traitant qui n'est pas établi sur le territoire de l'Union[74], ce dernier doit désigner par écrit un représentant dans l'Union[75]. Le représentant est la personne à qui, notamment, les autorités de contrôle et les personnes concernées doivent s'adresser, en plus ou à la place du responsable du traitement ou du sous-traitant, pour toutes les questions relatives au traitement, aux fins d'assurer le respect du présent règlement[76]. L'obligation de mandater un représentant ne s'applique pas lorsque le traitement est occasionnel, qu'il n'implique pas de traitement à grande échelle de catégories particulières de données ou des données relatives à des condamnations pénales ou des infractions, et qu'il n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement. Cette obligation ne s'applique pas non plus aux autorités publiques et autres organismes publics[77].

F) Le sous-traitant

31. Le sous-traitant est celui qui traite des données pour compte du responsable du traitement. Lorsque ce dernier fait appel à ce type de prestataires, il ne peut choisir qu'un sous-traitant qui présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement soit conforme aux règles fixées par le Règlement et que la protection des droits de la personne concernée soit garantie[78]. Il est maintenant précisé que le sous-

[74] C'est-à-dire lorsque les traitements sont liés à l'offre de biens ou de services à des personnes concernées dans l'Union ou au suivi du comportement de personnes concernées dans l'Union (*cf.* art. 3.2 du Règlement).

[75] Art. 27.1 du Règlement. Le représentant doit être établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi.

[76] Voy. art. 27.3 du Règlement. La désignation d'un représentant par le responsable du traitement ou le sous-traitant est sans préjudice d'actions en justice qui pourraient être intentées contre le responsable du traitement ou le sous-traitant lui-même (art. 27.5 du Règlement).

[77] Voy. art. 27.2 du Règlement.

[78] Voy. art. 28.1 du Règlement. Le respect, par le sous-traitant, d'un code de conduite approuvé ou le recours à un mécanisme de certification approuvé peut servir d'élément pour démontrer l'existence de garanties suffisantes (art. 28.5 du Règlement).

traitant ne peut pas faire appel à un autre sous-traitant sans l'autorisation écrite, préalable, spécifique ou générale, du responsable du traitement[79].

Le traitement de données en sous-traitance doit être régi par un contrat ou tout autre acte juridique au titre du droit de l'Union ou d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement. Ce contrat doit définir l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement[80].

Lorsqu'un sous-traitant recrute un autre sous-traitant (un sous-traitant en seconde ligne) pour mener des activités de traitement spécifiques

[79] Art. 28.2 du Règlement. Dans le cas d'une autorisation écrite générale, le sous-traitant doit informer le responsable du traitement de tout changement concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

[80] Sans préjudice du recours à des clauses contractuelles types, l'article 28.3 détaille ce que ce contrat (sous forme écrite ou électronique) ou cet acte juridique doit contenir :

1° le traitement ne se fait que sur instruction documentée du responsable du traitement, en ce compris les transferts de données, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis. Dans ce cas, le sous-traitant doit en informer le responsable du traitement avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

2° l'obligation du sous-traitant de veiller à ce que les personnes autorisées à traiter les données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

3° l'obligation du sous-traitant de prendre toutes les mesures requises en matière de sécurité des données ;

4° lorsqu'il recrute un sous-traitant en seconde ligne, le premier sous-traitant doit respecter les mêmes conditions que celles imposées au responsable du traitement pour recruter un sous-traitant et ce sous-traitant en seconde ligne doit être tenu aux mêmes obligations que le premier sous-traitant ;

5° le sous-traitant doit tenir compte de la nature du traitement et il doit aider le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits ;

6° le sous-traitant doit aider le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du Règlement, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

7° selon le choix du responsable du traitement, le sous-traitant doit supprimer toutes les données ou les renvoyer au responsable du traitement au terme de la prestation de services, et détruire toutes les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données ;

8° le sous-traitant doit mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations imposées en matière de sous-traitance de données et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il aurait mandaté, et contribuer à ces audits.

pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles imposées au premier sous-traitant doivent être imposées à cet autre sous-traitant[81]. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations[82]. Si, en violation du Règlement, un sous-traitant détermine les finalités et les moyens du traitement, il est considéré comme un responsable du traitement pour ce traitement[83], avec toutes les conséquences qui s'y attachent en termes de sanction et sans préjudice du droit de la personne concernée de le poursuivre en réparation de son préjudice.

G) Le principe du traitement sous l'autorité du responsable du traitement ou du sous-traitant

32. En règle, le sous-traitant et toute personne qui agit sous l'autorité du responsable du traitement ou du sous-traitant et qui a accès à des données, ne peut pas traiter ces données, sauf sur instruction du responsable du traitement, à moins d'y être obligé par le droit de l'Union ou le droit d'un État membre[84].

H) Le registre des activités de traitement

33. De manière fort regrettable et par un manque de compréhension de son utilité dans la mise en œuvre des droits de la personne concernée, notamment, le Règlement n'a pas maintenu l'obligation de tenir un registre public des traitements automatisés de données que tout un chacun pouvait consulter facilement en ligne. Ce registre public est remplacé par un registre tenu par chaque responsable de traitement[85], c'est-à-dire qu'un registre unique et public est remplacé par une multitude de registres privés et dont l'accès n'est pas libre. De plus,

---

[81] Ce qui doit se faire par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement.

[82] Art. 28.4 du Règlement.

[83] Voy. art. 28.10 du Règlement.

[84] Art. 29 du Règlement.

[85] Voy. art. 30 du Règlement. Ce registre peut être sous forme écrite ou électronique. Il doit être mis à la disposition de l'autorité de contrôle sur demande.

cette obligation ne s'applique pas à l'entreprise ou l'organisation qui compte moins de deux cent cinquante employés sauf si le traitement est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, ou si le traitement n'est pas occasionnel ou s'il porte, notamment, sur les catégories particulières de données ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions[86].

Le registre à tenir par chaque responsable de traitement doit contenir toutes les informations suivantes :

1) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

2) les finalités du traitement ;

3) une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

4) les catégories de destinataires auxquels les données ont été ou seront communiquées, en ce compris les destinataires dans des pays tiers ou des organisations internationales ;

5) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, en ce compris l'identification de ce pays tiers ou de cette organisation internationale et, s'il échet, les documents attestant de l'existence de garanties appropriées ;

6) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;

7) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles requises.

De même, et sous les mêmes conditions que le responsable de traitement, chaque sous-traitant et, le cas échéant, le représentant du sous-traitant, doivent tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement. Ce registre doit comprendre :

1) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

2) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

[86] Voy. art. 30.5 du Règlement.

3) le cas échéant, les transferts de données vers un pays tiers ou à une organisation internationale, en ce compris l'identification de ce pays tiers ou de cette organisation internationale et, s'il échet, les documents attestant de l'existence de garanties appropriées ;

4) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles requises.

I) La coopération avec l'autorité de contrôle

34. Le responsable du traitement et le sous-traitant ainsi que, le cas échéant, leurs représentants, doivent coopérer avec l'autorité de contrôle, à la demande de celle-ci, dans l'exécution de ses missions[87].

J) La sécurité du traitement des données

35. Au titre de la sécurité des données, le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque lié à leur traitement. Ils doivent tenir compte à cet égard de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement de données ainsi que des risques (dont le degré de probabilité et de gravité varie) pour les droits et libertés des personnes physiques. Lors de l'évaluation du niveau de sécurité du traitement, il faut tenir compte, en particulier, des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite[88]. Les mesures qui permettent d'assurer le niveau de sécurité approprié peuvent consister, entre autres, en :

1) une pseudonymisation et un chiffrement les données ;

2) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

---

[87] Art. 31 du Règlement. L'application d'un Code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir d'élément pour démontrer le respect des exigences en matière de sécurité du traitement.

[88] Voy. art. 32 du Règlement.

3) des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

4) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement de données.

En tout cas, le responsable du traitement et le sous-traitant doivent prendre des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données, ne les traite pas, excepté sur instruction du responsable du traitement ou à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

K) La notification à l'autorité de contrôle des violations de données

36. Lorsqu'une violation de la sécurité entraîne, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non-autorisée de données transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données[89], le responsable du traitement doit notifier cet incident (appelé violation de données) à l'autorité de contrôle[90], dans les meilleurs délais et, si possible, trois jours au plus tard après en avoir pris connaissance[91]. Il est libéré de cette obligation de notifier l'incident si la violation de données n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Mais, dans tous les cas, le responsable du traitement doit documenter toute violation de données, en indiquant les faits concernant la violation des données, ses effets et les mesures prises pour y remédier. Cette documentation doit

[89] Voy. art. 4.12) du Règlement.

[90] La notification doit, à tout le moins :

1° décrire la nature de la violation de données, en ce compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données concernés ;

2° communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

3° décrire les conséquences probables de la violation de données ;

4° décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données, en ce compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

[91] Au-delà de ce délai, la notification doit être accompagnée des motifs du retard dans l'accomplissement de cette obligation. Si, et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

permettre à l'autorité de contrôle de vérifier le respect des obligations qui s'imposent en cas de violation de données. De la même façon, le sous-traitant doit notifier au responsable du traitement toute violation de la sécurité dans les meilleurs délais après en avoir pris connaissance. Il faut présumer qu'il est aussi tenu de documenter toute violation de données même si cela n'est pas expressément prévu.

L) La communication à la personne concernée d'une violation de données

37. De manière asymétrique par rapport à l'obligation de notification à l'autorité de contrôle, le responsable du traitement ne doit communiquer la violation de données à la personne concernée que dans l'hypothèse où elle est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. Cette communication doit alors intervenir dans les meilleurs délais. Elle doit décrire en des termes simples et clairs la nature de la violation des données intervenue, contenir le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, une description des conséquences probables de la violation de données, une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données, en ce compris, le cas échéant, les mesures pour en atténuer les conséquences négatives éventuelles. Toutefois, même en cas de risque élevé pour les droits et libertés, cette communication n'est pas nécessaire dans l'une des hypothèses suivantes :

1) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données affectées par la violation, en particulier les mesures qui rendent les données incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

2) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;

3) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Si le responsable du traitement n'a pas déjà communiqué la violation de données à la personne concernée, l'autorité de contrôle peut, après avoir examiné si cette violation de données est susceptible d'engendrer

un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que le responsable du traitement se trouve dans une des hypothèses où il en est exempté[92].

M) L'analyse de l'impact des opérations de traitement envisagés sur la protection des données

38. Le responsable du traitement doit effectuer une analyse de l'impact des opérations de traitement envisagées sur la protection des données lorsque le type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques[93]. L'analyse d'impact est, en tout cas, obligatoire dans les hypothèses suivantes :

1) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, en ce compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

---

[92] Art. 34 du Règlement.

[93] Voy. art. 35 du Règlement. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires. Le responsable du traitement doit demander conseil au délégué à la protection des données quand il effectue une telle analyse d'impact relative à la protection des données (dans la mesure où un tel délégué a été désigné – ce qui laisse ouverte la question de l'obligation de le faire lorsque le responsable du traitement n'avait pas d'obligation (formelle ou dans le cadre des mesures techniques et organisationnelles) d'en désigner un mais qu'il l'a quand même fait). L'autorité de contrôle doit établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise. L'autorité de contrôle communique ces listes au *Comité européen de la protection des données*. L'autorité de contrôle peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise. L'autorité de contrôle communique cette liste au *Comité européen de la protection des données*. Avant d'adopter ces deux sortes de listes, l'autorité de contrôle compétente doit appliquer le mécanisme de contrôle de la cohérence lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union. Le respect de codes de conduite approuvés doit être pris en compte lors de l'évaluation de l'impact des opérations de traitement, en particulier aux fins d'une analyse d'impact relative à la protection des données. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

2) le traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions ;

3) la surveillance systématique à grande échelle d'une zone accessible au public.

L'analyse de l'impact des opérations de traitement envisagés doit contenir les éléments suivants au minimum :

1) une description systématique des opérations de traitement envisagées et des finalités du traitement, en ce compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

2) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

3) une évaluation des risques pour les droits et libertés des personnes concernées ;

4) les mesures envisagées pour faire face aux risques, en ce compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Quand le traitement est nécessaire à l'exécution d'une obligation légale à laquelle le responsable du traitement est soumis ou lorsqu'il 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, qu'il a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis et que ce droit règlemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, aucune autre analyse d'impact n'est requise à moins que les États membres estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.

Si nécessaire, le responsable du traitement doit procéder à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

N) La consultation préalable et obligatoire de l'autorité de contrôle

39. Avant de mettre en œuvre le traitement, le responsable du traitement est obligé de consulter l'autorité de contrôle lorsque l'analyse d'impact indique que le traitement pourrait présenter un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque[94]. Lorsque l'autorité de contrôle est d'avis que le traitement est de nature à constituer une violation du Règlement, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, elle fournit par écrit, dans un délai maximum de huit semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage de ses pouvoirs d'enquête, d'imposer des mesures correctrices, d'autorisation et de consultation ou de tout autre pouvoir qui lui serait conféré par son droit national[95]. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant, de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation[96].

---

[94] Le responsable du traitement doit communiquer à l'autorité de contrôle les éléments suivants :

1° le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous- traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;

2° les finalités et les moyens du traitement envisagé ;

3° les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées ;

4° le cas échéant, les coordonnées du délégué à la protection des données ;

5° l'analyse d'impact relative à la protection des données ;

6° et toute autre information que l'autorité de contrôle pourrait demander.

[95] Voy. art. 58 du Règlement.

[96] Art. 36 du Règlement. Les États membres sont obligés de consulter l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement. De plus, le droit des États membres peut exiger que les responsables du traitement soient obligés de consulter l'autorité de contrôle et d'obtenir son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, en ce compris le traitement dans le cadre de la protection sociale et de la santé publique.

O) Le délégué à la protection des données

1° L'obligation de désigner un délégué à la protection des données

40. L'obligation de désigner un délégué à la protection des données est une des mesures qui a particulièrement retenu l'attention. Au-delà de l'hypothèse où cette désignait est requise au titre des mesures organisationnelles destinées à garantir la sécurité et la confidentialité des traitements de données, le responsable du traitement et le sous-traitant sont, en tout état de cause, obligés de désigner un délégué à la protection des données[97] dans trois hypothèses[98] :

1) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle[99] ;

2) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

3) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

---

[97] Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions qui lui incombent. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

[98] Voy. art. 37 du Règlement. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'il soit facilement joignable à partir de chaque lieu d'établissement. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille. Lorsqu'il n'y est pas formellement contraint, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

[99] Il demeure à trouver une justification à cette discrimination d'autant plus étonnante à l'heure où la justice tente de rejoindre le 21e siècle.

2° La fonction du délégué à la protection des données

41. La fonction du délégué à la protection des données obéit à des règles destinées à lui permettre d'exercer pleinement et effectivement sa mission :

1) La participation au processus décisionnel et opérationnel : le délégué à la protection des données doit être associé tant par le responsable du traitement que par le sous-traitant, et d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ;

2) La mise à disposition des ressources nécessaires : le responsable du traitement et le sous-traitant doivent aider le délégué à la protection des données à exercer ses missions en lui fournissant les ressources nécessaires pour exercer à cet effet, ainsi que l'accès aux données et aux opérations de traitement, et en lui permettant d'entretenir ses connaissances spécialisées ;

3) L'indépendance et la protection de la fonction : le responsable du traitement et le sous-traitant doivent veiller à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

4) L'absence de filtrage par rapport aux personnes concernées : les personnes concernées peuvent prendre directement contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données et à l'exercice de leurs droits.

5) La confidentialité de la fonction : le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.

6) La protection contre le caractère non-exclusif de la fonction : le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts[100].

[100] Voy. art. 38 du Règlement.

3° Les missions du délégué à la protection des données

42. Les missions qui incombent au délégué à la protection des données sont au moins les suivantes[101] :

1) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement et d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données ;

2) contrôler le respect des règles applicables en matière de protection des données, que ce soient les règles issues du Règlement, d'autres dispositions du droit de l'Union ou du droit des États membres ainsi que les règles internes du responsable du traitement ou du sous-traitant, en matière de protection des données, en ce compris la question de la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

3) dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci ;

4) coopérer avec l'autorité de contrôle ;

5) faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, en ce compris à propos de sa consultation préalable, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données doit tenir compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

§ 9. Les transferts de données vers des pays tiers ou des organisations internationales

A) Le principe général applicable aux transferts de données vers des pays tiers ou des organisations internationales

43. L'idée de base qui gouverne les règles applicables aux transferts de données vers un pays tiers ou une organisation internationale est que le niveau de protection des personnes physiques garanti par le Règlement

[101] Voy. art. 39 du Règlement.

ne soit pas compromis. Globalement, le transfert de données doit être conforme à l'ensemble des dispositions du Règlement, d'une part, et, d'autre part, il doit respecter, en outre, les règles propres aux transferts de données vers un pays tiers ou une organisation internationale[102].

B) Les décisions d'adéquation

44. Tout d'abord, un transfert de données vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question, assure un niveau de protection adéquat. Dans ce cas, le transfert de données ne nécessite pas d'autorisation spécifique[103].

C) Les garanties appropriées

45. En l'absence d'une décision d'adéquation de la Commission européenne, le responsable du traitement ou le sous-traitant ne peuvent transférer des données que s'il a prévu des garanties appropriées et que les personnes concernées disposent de droits opposables et de voies de droit effectives[104].

D) Les transferts ou divulgations non autorisées par le droit de l'Union

46. Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition

[102] Voy. le libellé de l'article 44 du Règlement qui appelle certainement d'autres développements. Voy. aussi l'article 50 du Règlement à propos de la coopération internationale dans le domaine de la protection des données.

[103] Voy. art. 45.1 du Règlement. L'article 45.2 du Règlement énumère les critères à prendre en considération afin d'évaluer le niveau d'adéquation. La Commission publie au Journal officiel de l'Union européenne et sur son site internet une liste des pays tiers, des territoires et des secteurs déterminés dans un pays tiers et des organisations internationales pour lesquels elle a constaté par voie de décision qu'un niveau de protection adéquat est ou n'est plus assuré.

[104] Voy. art. 46 du Règlement qui énonce aussi les manières de fournir les garanties appropriées comme des règles d'entreprise contraignantes (voy. art. 47 du Règlement à leur propos), des clauses types de protection des données, un code de conduite approuvé, un mécanisme de certification ou des clauses contractuelles.

qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert prévus dans les règles propres applicables aux transferts de données vers un pays tiers ou une organisation internationale[105].

E) Les dérogations pour des situations particulières

47. En l'absence de décision d'adéquation et de garanties appropriées, le transfert de données vers un pays tiers ou une organisation internationale est néanmoins possible dans les hypothèses détaillées dans le Règlement[106].

§ 10. Les droits reconnus à la personne concernée

48. Si la directive 95/46/CE ne reconnaissait formellement que trois droits à la personne concernée (le droit d'accès, le droit de s'opposer au traitement de données et le droit de ne pas être soumis à des décisions individuelles automatisées), le Règlement lui en reconnaît huit (le droit à l'information, le droit d'accès, le droit à la rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit à la portabilité des données, le droit de s'opposer au traitement de données et le droit de ne pas être soumis à des décisions individuelles automatisées) sans qu'il ne soit possible de prédire si cette augmentation formelle de leur nombre va induire une augmentation de la protection des données et une plus grande participation des individus à la société de l'information[107].

---

[105] Art. 48 du Règlement.

[106] Voy. art. 49 du Règlement. Dans le cadre de l'exercice de leurs prérogatives de puissance publique, les autorités publiques ne peuvent pas recourir au consentement explicite de la personne concernée, ni à l'hypothèse de l'exécution du contrat ou à la mise en œuvre de mesures précontractuelles pas plus qu'à celle de la conclusion et de l'exécution du contrat conclu dans l'intérêt de la personne concernée. Par ailleurs, en l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres notifient de telles dispositions à la Commission.

[107] Voy. les limitations qui peuvent être apportées à ces droits par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis, par la voie de mesures législatives, conformément à l'article 23 du Règlement. Ces limitations ne sont admissibles que si elles respectent l'essence des libertés et droits fondamentaux et qu'elles constituent des mesures nécessaires et proportionnées dans une société démocratique pour garantir l'un des objectifs énumérés par cette disposition.

A) Le principe de la transparence

49. La transparence est un principe de base de la protection des données. Sans transparence, il n'est pas possible de mettre en œuvre la protection des données, que ce soit dans le chef de la personne concernée ou des autorités. Le Règlement insiste, à juste titre, sur les conséquences qu'il faut en tirer[108].

D'abord, lorsque le responsable du traitement doit communiquer de l'information à la personne concernée, il doit le faire d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour les informations spécifiquement destinées aux enfants. Ces informations doivent être fournies par écrit ou par d'autres moyens y compris par voie électronique quand c'est approprié. Mais la personne concernée peut demander que ces informations lui soient fournies oralement. Dans ce cas, le responsable du traitement doit s'assurer de l'identité de la personne concernée autrement que par une déclaration orale de celle-ci (quoique cela puisse bien vouloir dire).

Ensuite, le responsable du traitement doit faciliter l'exercice des droits de la personne concernée. À propos des traitements qui ne requièrent pas l'identification de la personne concernée, le responsable du traitement ne peut pas refuser de donner suite à une demande d'exercice des droits sauf s'il démontre qu'il n'est pas en mesure d'identifier la personne concernée qui s'est adressée à lui[109].

En tout état de cause, le responsable du traitement doit informer la personne concernée des suites réservées à sa demande et ce, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande[110].

Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes[111].

Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque

[108] Voy. art. 12 du Règlement.

[109] La disposition veut sans doute dire s'il n'est pas en mesure d'identifier les données qui concernent la personne qui souhaite exercer ses droits puisque, s'il est approché par la personne concernée, le responsable du traitement connait nécessairement son identité.

[110] Quand le responsable du traitement a des doutes raisonnables sur l'identité de la personne concernée, il peut demander des informations supplémentaires nécessaires pour confirmer son identité (voy. art. 12.6 du Règlement).

[111] Le responsable du traitement doit informer la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il doit l'informer sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande, des motifs de son refus et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel.

La règle veut que l'information et l'exercice des droits la personne concernée soient gratuits dans le chef de celle-ci ; le responsable du traitement ne peut lui exiger aucun paiement à quelque titre que ce soit. Par contre, le responsable du traitement peut refuser de donner suite aux demandes manifestement infondées ou excessives (notamment en raison de leur répétition abusive) ou exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées[112].

B) Le droit à l'information

50. Comme la directive 95/46/CE, le Règlement distingue l'information due par le responsable du traitement à la personne concernée selon que les données sont ou non collectées auprès de la personne concernée. Dans les deux hypothèses, les informations à communiquer peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine[113].

1° Les informations à fournir lorsque les données sont collectées auprès de la personne concernée

51. Au moment même où les données sont obtenues auprès de la personne concernée, le responsable du traitement doit lui fournir un socle de base d'informations[114] auxquelles il faut ajouter les informations com-

[112] C'est au responsable du traitement de prouver le caractère infondé ou excessif de la demande formée par la personne concernée.

[113] Art. 12.7 du Règlement. En vertu de l'article 12.8 du Règlement, la Commission est habilitée à adopter des actes délégués aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées.

[114] Art. 13.1 du Règlement : le responsable du traitement doit fournir *toutes* les informations suivantes :

plémentaires qui seront nécessaires pour garantir un traitement équitable et transparent[115], sauf à ce que la personne concernée dispose déjà de ces informations[116].

1° l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
2° le cas échéant, les coordonnées du délégué à la protection des données ;
3° les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
4° lorsque le traitement est fondé sur l'intérêt légitime du traitement, l'indication des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers ;
5° les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent ; et
6° le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46, 47, ou 49.1, 2e alinéa, du Règlement, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

[115] Art. 13.2 du Règlement : le cas échéant, le responsable du traitement doit fournir les informations supplémentaires suivantes :
1° la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
2° l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
3° lorsque le traitement est fondé sur le consentement de la personne concernée (que ce soit pour des données ordinaires ou des catégories particulières de données), l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
4° le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
5° des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
6° l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

[116] Art. 13.4 du Règlement. Lorsqu'il a l'intention d'effectuer un *traitement ultérieur* des données à caractère personnel *pour une finalité autre* que celle pour laquelle les données à caractère personnel ont été collectées, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information complémentaire qui serait nécessaire (art. 13.3 du Règlement).

2° Les informations à fournir lorsque les données ne sont pas collectées auprès de la personne concernée

52. Le régime de l'information à fournir par le responsable du traitement à la personne concernée a été substantiellement revu[117]. Comme dans l'hypothèse précédente, le responsable du traitement doit fournir à la personne concernée un socle de base d'informations[118] auxquelles il faut ajouter les informations complémentaires qui seront nécessaires pour garantir un traitement équitable et transparent[119]. Ces informations doivent être fournies dans un délai raisonnable après avoir obtenu les

---

[117] Art. 14 du Règlement.

[118] Art. 14.1 du Règlement : le responsable du traitement doit fournir *toutes* les informations suivantes :

1° l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement ;
2° le cas échéant, les coordonnées du délégué à la protection des données ;
3° les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ;
4° les catégories de données à caractère personnel concernées ;
5° le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel ;
6° le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers ou une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46, 47 ou 49.1, 2e alinéa, du Règlement, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition.

[119] Art. 14.2 du Règlement : le cas échéant, le responsable du traitement doit fournir les informations supplémentaires suivantes :

1° la durée pendant laquelle les données à caractère personnel seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;
2° lorsque le traitement est fondé sur l'intérêt légitime du traitement, l'indication des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers ;
3° l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ainsi que du droit de s'opposer au traitement et du droit à la portabilité des données ;
4° lorsque le traitement est fondé sur le consentement de la personne concernée (que ce soit pour des données ordinaires ou des catégories particulières de données), l'existence du droit de retirer le consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
5° le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
6° la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public ;
7° l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

données à caractère personnel. Ce caractère raisonnable s'apprécie au regard des circonstances particulières dans lesquelles les données à caractère personnel sont traitées mais, en tout état de cause, il ne peut pas dépasser un mois. Dans l'hypothèse où les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, ces informations doivent lui être fournies au plus tard au moment de la première communication. S'il est envisagé de communiquer les informations à un autre destinataire, ces informations doivent lui être fournies au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois[120]. De manière regrettable, les possibilités de se soustraire à l'information de la personne concernée ont été maintenues et, dans une certaine mesure, élargies[121].

C) Le droit d'accès

53. Si le responsable du traitement est obligé de fournir de l'information à la personne concernée, celle-ci est aussi en droit de l'interpeller pour obtenir des informations sur le traitement de données qui la concernent[122] et pour obtenir l'accès aux données qui le concernent et

[120] Voy. art. 14.3 du Règlement. Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement doit, au préalable, fournir à la personne concernée des informations au sujet de cette autre finalité et toute autre information supplémentaire pertinente.

[121] Le responsable du traitement peut se soustraire à cette obligation, pourtant fondamentale, dans les hypothèses suivantes (art. 14.5 du Règlement) :

1° lorsque la personne concernée dispose déjà de ces informations ;

2° lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques sous réserve des conditions et garanties visées à l'article 89.1 du Règlement, ou dans la mesure où cette obligation est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles ;

3° lorsque l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée ;

4° ou lorsque les données à caractère personnel doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membre, y compris une obligation légale de secret professionnel.

[122] Il faut toutefois noter l'asymétrie dans le contenu de l'information selon qu'elle doit être fournie par le responsable du traitement ou qu'elle soit demandée par la personne concernée.

qui font l'objet d'un traitement. La première information que la personne concernée est en droit d'exiger du responsable du traitement est de savoir si des données qui la concernent font ou non l'objet d'un traitement. Dans l'affirmative, la personne concernée a le droit d'accéder aux données qui la concernent, ainsi que le droit d'obtenir des informations.

1° Les informations à fournir à la personne concernée

54. Si le responsable du traitement confirme à la personne concernée qu'il traite des données qui la concernent, celle-ci a le droit d'obtenir les informations suivantes[123] :

1) les finalités du traitement ;

2) les catégories de données à caractère personnel concernées ;

3) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales ;

4) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

5) l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;

6) le droit d'introduire une réclamation auprès d'une autorité de contrôle ;

7) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;

8) l'existence d'une prise de décision automatisée, y compris un profilage, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;

9) lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées prises en ce qui concerne ce transfert.

[123] Voy. art. 15.1 et 2 du Règlement.

2° Les modalités du droit d'accès

55. Il demeure à s'entendre sur ce que signifie accéder aux données ainsi que sur la manière d'exercer cet accès. Visiblement, il ne s'agit pas seulement du pouvoir d'en demander copie[124]. Par ailleurs, la personne concernée a le droit de demander et d'obtenir une copie des données traitées. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement. Le responsable du traitement ne peut pas exiger de paiement à ce titre sauf lorsque la personne concernée demande une copie supplémentaire. Dans ce cas, le responsable du traitement ne peut pas demander plus que le paiement de frais raisonnables tels que ceux-ci sont calculés sur base des coûts administratifs[125]. Le Règlement précise que le droit d'obtenir une copie des données ne doit pas porter atteinte aux droits et libertés d'autrui[126].

D) Le droit de rectification

56. La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données qui la concernent et qui sont inexactes. Compte tenu des finalités poursuivies par leur traitement, la personne concernée a le droit d'obtenir que les données incomplètes soient complétées, y compris en fournissant une déclaration complémentaire[127].

[124] En effet, l'article 15.4 du Règlement énonce que « [l]e droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui », ce qui signifie que le droit à la copie ne se confond pas avec le droit visé à l'article 15.1 du Règlement.

[125] Art. 15.3 du Règlement.

[126] Art. 15.4 du Règlement.

[127] Art. 16 du Règlement. Autrement dit, la personne concernée est associée à la réalisation des finalités poursuivies par le responsable du traitement, ce qui induit, quelque part, un renversement des rôles. Le responsable du traitement doit notifier à chaque destinataire auquel les données ont été communiquées toute rectification effectuée, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement doit fournir à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande (art. 19 du Règlement).

E) Le droit à l'effacement ou à l'oubli

1° Le principe

57. Présenté comme une avancée significative apportée par le Règlement à la protection des données, le droit à l'effacement ou à l'oubli préexistait toutefois dans la directive 95/46/CE en tant que conséquence logique et, en principe, implacable, de la limite imposée au responsable du traitement dans la durée conservation des données sous une forme permettant l'identification de la personne concernée au terme de la réalisation des finalités poursuivies. Maintenant, la personne concernée se voit reconnaître expressément le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, des données qui la concernent, dans l'une des hypothèses suivantes, étant entendu que lorsqu'elle exerce ce droit, le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais[128] :

1) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;

2) la personne concernée a retiré son le consentement et qu'il n'existe pas d'autre fondement juridique au traitement ;

3) la personne concernée s'oppose au traitement pour des raisons tenant à sa situation particulière et il n'existe pas de motif légitime impérieux pour poursuivre le traitement, ou la personne concernée s'oppose au traitement à des fins de prospection ;

4) les données à caractère personnel ont fait l'objet d'un traitement illicite ;

5) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;

6) les données à caractère personnel ont été collectées dans le cadre de l'offre directe de services de la société de l'information aux enfants.

2° Les effacements subséquents et par ricochet

58. Lorsqu'il a rendu publiques les données et qu'il est tenu de les effacer, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, doit prendre des mesures raisonnables, y

[128] Art. 17.1 du Règlement.

compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci[129].

3° Les exceptions au droit à l'effacement ou à l'oubli

59. Même lorsque le traitement des données est inutile, dépourvu de fondement juridique, dépourvu de nécessité impérieuse, illicite, et même lorsque la loi impose l'effacement des données, la personne concernée se voit dénier, de manière surprenante et paradoxale, le droit à l'effacement ou à l'oubli des données qui la concernent lorsque le traitement est nécessaire[130] :

1) à l'exercice du droit à la liberté d'expression et d'information ;

2) pour respecter une obligation légale qui impose le traitement et qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

3) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;

4) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89.1 du Règlement, dans la mesure où le droit à l'effacement ou à l'oubli est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de ce traitement ;

5) ou à la constatation, à l'exercice ou à la défense de droits en justice.

[129] Art. 17.2 du Règlement. Le responsable du traitement doit notifier à chaque destinataire auquel les données ont été communiquées tout effacement de données effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande (art. 19 du Règlement).

[130] Voy. art. 17.3 du Règlement.

F) Le droit à la limitation du traitement

60. Afin de donner un peu de crédibilité à l'effectivité des droits de la personne concernée, celle-ci a le droit d'exiger et d'obtenir du responsable du traitement qu'il limite le traitement des données qui la concernent dans les hypothèses suivantes[131] :

1) lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée et ce, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;

2) lorsque le traitement est illicite et que la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;

3) lorsque le responsable du traitement n'a plus besoin des données mais que celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;

4) lorsque la personne concernée s'est opposée au traitement pour des raisons tenant à sa situation particulière et ce, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement ne prévaudraient pas sur ceux de la personne concernée.

G) Le droit à la portabilité des données

61. Lorsque les données sont traitées sur base de son consentement ou d'un contrat, et à l'aide de procédés automatisés, la personne concernée a le droit de demander et de recevoir du responsable du traitement, dans un format structuré, couramment utilité et lisible par machine, les données qu'elle lui a fournies. La personne concernée peut, ensuite, les transmettre à un autre responsable du traitement. Elle peut aussi demander au premier

[131] Art. 18 du Règlement. Lorsque le traitement a été limité, ces données ne peuvent, à l'exception de la conservation, être traitées qu'avec le consentement de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice, ou pour la protection des droits d'une autre personne physique ou morale, ou encore pour des motifs importants d'intérêt public de l'Union ou d'un État membre. Le responsable du traitement ne peut lever la limitation au traitement qu'après en avoir informé la personne concernée. Par ailleurs, le responsable du traitement doit notifier à chaque destinataire auquel les données à caractère personnel ont été communiquées toute limitation du traitement effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés. Le responsable du traitement fournit à la personne concernée des informations sur ces destinataires si celle-ci en fait la demande (art. 19 du Règlement).

responsable du traitement de les transmettre directement à un autre responsable du traitement si la technique le permet[132].

H) Le droit d'opposition

62. La personne concernée dispose du droit, spécial, de s'opposer au traitement de ses données pour des raisons tenant à sa situation particulière, et elle dispose du droit, général, de s'opposer au traitement de ses données à des fins de prospection. L'existence de ce double droit est explicitement portée à l'attention de la personne concernée, au plus tard au moment de la première communication avec la personne concernée. Il doit lui être présenté clairement et séparément de toute autre information[133].

1° Le droit de s'opposer au traitement de données pour des raisons tenant à la situation particulière de la personne concernée

63. Comme auparavant sous la directive 95/46/CE, la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données ou un profilage réalisé dans le cadre de l'exécution d'une mission d'intérêt public ou qui relève de l'exercice de l'autorité publique dont est investi le responsable du traitement[134]. La personne concernée peut aussi s'opposer au traitement de données ou au profilage réalisé dans la poursuite des intérêts légitimes du responsable du traitement ou d'un tiers. Suite à l'opposition de la personne concernée, le responsable du traitement ne peut plus traiter les données, à moins qu'il ne démontre l'existence de motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la

[132] Voy. art. 20 du Règlement. Ce droit est sans préjudice du droit à l'effacement ou à l'oubli. Ce droit ne s'applique pas au traitement 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. Il ne peut pas non plus porter atteinte aux droits et libertés de tiers.

[133] Voy. art. 21 du Règlement. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer son droit d'opposition à l'aide de procédés automatisés utilisant des spécifications techniques.

[134] Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public (voy. art. 21.6 du Règlement).

personne concernée, ou que le traitement est nécessaire pour la constatation, l'exercice ou la défense de droits en justice.

2° Le droit de s'opposer au traitement de données à des fins de prospection

64. La personne concernée a le droit de s'opposer à tout moment, et sans avoir à se justifier, au traitement des données qui la concernent ou au profilage réalisé dans une finalité de prospection. Lorsque la personne concernée s'oppose au traitement à des fins de prospection, les données à caractère personnel ne sont plus traitées à ces fins.

I) Le droit de ne pas être soumis à une décision individuelle automatisée en ce compris au profilage

65. La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, en ce compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire[135]. Ce droit ne peut pas être invoqué lorsque la décision automatisée[136] :

1) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ;

2) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ;

3) ou est fondée sur le consentement explicite de la personne concernée.

Lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement ou lorsque la décision est fondée sur le consentement explicite de la personne concernée, le responsable du traitement doit mettre en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins le droit d'obtenir une

[135] Voy. art. 22 du Règlement.

[136] Toutefois, les décisions automatisées ne peuvent pas se fonder sur les catégories particulières de données, à moins que (1) la personne concernée n'ait donné son consentement explicite ou que le traitement ne soit le traitement nécessaire pour des motifs d'intérêt public important et (2) que, dans les deux hypothèses, des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée soient mise en œuvre.

intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

J) La mise en place d'organes, de procédures et de sanctions spécifiques

66. Dans la droite ligne de ce qui avait été prévus dès l'origine mais de manière plus complète et plus élaborée, le Règlement prévoit des organes, des procédures et des sanctions spécifiques afin d'assurer l'effectivité du cadre juridique qui encadre les traitements de données et les droits des personnes concernées.

Ainsi, chaque État membre de disposer d'une ou plusieurs autorités publiques *indépendantes* charges de surveiller l'application du Règlement afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de données et de faciliter le libre flux des données au sein de l'Union[137].

Le Règlement remplace le Groupe de travail de l'article 29 par le Comité européen de la protection des données. Le Secrétariat du Comité est assuré par le Contrôleur européen de la protection des données.

Enfin, la protection des données doit se développer dans un cadre juridique qui soit à la fois effectif et coercitif, c'est-à-dire qui permette de contraindre les individus, les entreprises et les autorités publiques à se soumettre à ses règles. À cet effet, la personne concernée a le droit de saisir l'autorité de contrôle compétente d'une violation de la protection des données à propos d'un traitement qui la concerne. Par ailleurs, un recours

[137] Voy. art. 51 du Règlement sur le principe de l'indépendance et l'article 55 du Règlement sur la question des compétences de l'autorité de contrôle (elle est compétente pour le territoire de l'État membre dont elle relève) (pour les traitements nécessaires pour le respect d'une obligation légale à laquelle le responsable du traitement est soumis ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, c'est l'autorité de contrôle de l'État membre concerné qui est compétente et l'article 56 du Règlement ne s'applique pas à propos de la compétence de l'autorité de contrôle chef de file). Conformément à l'article 4.22 du Règlement, une autorité de contrôle est concernée lorsque :

1° le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;

2° des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ;

3° une réclamation a été introduite auprès de cette autorité de contrôle.

Il est, par ailleurs, expressément prévu que les autorités de contrôle ne sont pas compétentes pour contrôler les opérations de traitement effectuées par les juridictions dans l'exercice de leur fonction juridictionnelles (art. 55.3 du Règlement). Les missions et les pouvoirs des autorités de contrôle sont détaillés aux articles 57 et 58 du Règlement.

peut être introduit contre l'autorité de contrôle ainsi que contre un responsable du traitement ou un sous-traitant. La personne concernée a le droit d'être indemnisée en cas de dommage et l'autorité de contrôle peut infliger des amendes administratives au responsable du traitement ou au sous-traitant. En tout état de cause, chaque État membre doit mettre en place des sanctions effectives, proportionnées et dissuasives pour les violations de la protection des données.

Conclusions

Sous l'angle de la question de la vulnérabilité[138], le premier constat à dresser en matière de protection des données serait celui d'une vulnérabilité généralisée de toutes les personnes physiques[139] face au développement des technologies de l'information et de la communication. Ces dernières constitueraient autant de menaces pour leurs droits et libertés. Ce constat, qui rejoint en quelque sorte la volonté, compréhensible, de ne plus concevoir la vulnérabilité en termes de discrimination ou de stigmatisation, est néanmoins problématique. En effet, quel est l'intérêt de recourir à une qualification qui s'applique à tout le monde, sans exception, puisque les qualifications servent justement à distinguer la situation des uns des autres afin de leur appliquer un régime juridique différencié ? Ensuite, si chacun est, on a presque envie de dire « par nature », vulnérable face aux technologies de l'information et de la communication, cette vulnérabilité n'est toutefois pas identique ; elle ne concerne peut-être pas tout le monde, peut-être pas tous et toutes de la même façon et peut-être pas tous et toutes avec les mêmes conséquences. Autrement dit, si chacun est vulnérable, la catégorisation interviendra alors de toute

[138] Le concept de vulnérabilité n'est pas univoque ni neutre : il peut être compris et utilisé de manière très différente ; il est donc aussi susceptible de nourrir de très nombreuses controverses. Voy. déjà : M. Blondel, *La personne vulnérable en droit international*, Thèse de doctorat, Université de Bordeaux, 2015 ; L. Dutheil-Warolin, *La notion de vulnérabilité de la personne physique en droit privé*, thèse de doctorat, Université de Limoges, 2004 ; B. Eyraud et P. Vidal-Naquet, « La vulnérabilité saisie par le droit », *Revue Justice Actualités*, 2013, p. 3 ; M. A. Fineman, « The Vulnerable Subject : Anchoring Equality in the Human Condition », *Yale Journal of Law & Feminism*, 2008, vol. 20, issue 1, art. 2 ; M.A. Fineman et A. Grear (ed.), *Vulnerability : Reflections on a New Ethical Foundation for Law and Politics*, Ashgate Pub. Co., 2013 ; N.A. Kohn, « Vulnerability Theory and the Role of Government », *Yale Journal of Law & Feminism*, 2014, vol. 26, issue 1, article 2.

[139] En présence d'une exclusion formelle des personnes morales qui doivent trouver une protection par ailleurs comme celle de leurs secrets d'affaires ou en matière de perquisitions.

façon dans un deuxième temps lorsqu'il s'agira de mettre en œuvre une véritable politique de protection qui elle sera différenciée.

Ceci d'autant plus que, quelque part, le Règlement lui-même ne semble pas considérer les personnes majeures concernées par le traitement de données à caractère personnel comme étant nécessairement vulnérables puisqu'il instaure un régime de quasi-autorisation de traitement sous réserve de respecter les principes applicables aux traitements de données ainsi que les obligations générales à charge du responsable du traitement et du sous-traitant éventuel.

Par contre, le Règlement général sur la protection des données distingue les données « ordinaires » des catégories « particulières » de données. Ainsi, le traitement de données qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, est interdit sauf exceptions. Dans le même ordre d'idées, le traitement des données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes, fondé sur l'article 6.1 du Règlement, ne peut être effectué que sous le contrôle de l'autorité publique ou que si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées.

De même, le Règlement fixe aussi des conditions extraordinaires pour reconnaître la validité du consentement de la personne aux traitements de données à caractère personnel qui la concernent, ainsi que des règles particulières pour le consentement relatif aux enfants mineurs d'âge.

En conséquence, les personnes concernées par des catégories particulières de données à caractère personnel ainsi que les personnes mineures d'âge semblent d'office être vulnérables.

Toute la question consiste alors à s'interroger sur l'opportunité d'analyser la protection des données sous l'angle de la vulnérabilité des personnes concernées – sans compter le fait que d'aucun pourrait refuser de voir sa situation envisagée sous cet angle, d'autant que la protection des données poursuit aussi l'objectif d'armer le citoyen dans la société de l'information face à ce qui pourrait être fait des données qui le concernent et à lui fournir des moyens pour en contrôler l'usage (que ce soit par la possibilité de consentir au traitement de données qui le concernent ou d'accéder aux données qui le concernent et qui font l'objet d'un traitement de données) – c'est le droit à l'autodétermination informationnelle

et la « mise en capacité » (ou « autonomisation » ou « empowerment ») des citoyens.

En réalité, la protection des données balance entre la protection au sens strict (la protection contre les dangers liés aux technologies de l'information et de la communication que ce soit en raison du contenu informationnel des catégories particulières de données ou de l'âge de la personne concernée) et la possibilité pour l'individu de participer de manière autonome aux activités de la société de l'information. Mais, pour atteindre ce second objectif, encore faudrait-il que les politiques menées au niveau fédéral ou au niveau des entités fédérées multiplient toujours plus les opportunités permettant aux citoyens d'être des sujets actifs de la société de l'information et pas seulement ses victimes, ce qui est encore loin de correspondre à la réalité sur le terrain comme l'ont démontré les récents scandales (par exemple, celui de *Cambridge Analytica*).