PROTECTION DES DONNÉES PERSONNELLES : CONCILIATION AVEC D'AUTRES DROITS FONDAMENTAUX

Par Nelson Rodrigues

I PARCOURS HISTORIQUE ET CADRE NORMATIF 1. Origine et évolution 2. Encadrement de la problématique II CONCILIATION AVEC D'AUTRES DROITS FONDAMENTAUX 1. Liberté d'expression et d'accès à l'information 1.1. Signification et contours jurisprudentiels 1.2. Problèmes posés par la Directive 95/46/CE 1.3. Conciliation avec la protection des données personnelles 1.3.1. Liberté d'expression 1.3.2. Accès à l'information 2. Droit de propriété 2.1. Protection nationale et internationale 2.2. Propriété intellectuelle, réseaux P2P et protection des données personnelles 2.2.1. Description de la problématique 2.2.2. Base juridique légitimant l'intrusion 2.2.3. Validité de l'intrusion 2.3. Protection à travers l'art. 7/f) de la Directive 95/46/CE 2.4. Nouveautés apportées par le Règlement 3. Liberté d'entreprise 3.1. Contexte 3.2. Légalité du traitement 3.2.1. Légitimation du traitement 3.2.2. Devoir d'information et principe de qualité 3.2.3. Dispositions additionnelles contenues dans le Règlement 3.3. Jurisprudence de la CeDH III CONCLUSIONS 1. Sur la jurisprudence de la CJUE et de la CEDH 2. Sur les contributions du Règlement

---

Résumé : Le présent article a pour objectif d'illustrer la conciliation entre le droit à la protection des données personnelles et d'autres droits fondamentaux. L'analyse est centrée sur les dispositions de la Directive 95/46/CE, la jurisprudence de la Cour de Justice de l'Union Européenne et de la Cour Européenne des Droits de l'Homme ainsi que les nouveautés introduites par le Règlement (UE) 2016/679.

Mots-clefs : protection des données personnelles, liberté d'expression, accès à l'information, droit de propriété, liberté d'entreprise, Directive 95/46/CE, Règlement (UE) 2016/679

Abstract: The aim of this article is to illustrate the conciliation between the right to data protection and other fundamental rights. The provisions of Directive 95/46/EC, the case law of the European Court of Justice and the European Court of Human Rights as well as the new arrangements introduced by Regulation (EU) 2016/679 constitute the main sources of this work.

Keywords: protection of personal data, freedom of expression and information, right to property, freedom to conduct a business, Directive 95/46/EC, Regulation (EU) 2016/679

I PARCOURS HISTORIQUE ET CADRE NORMATIF

1. Origine et évolution

Tant l'origine que l'évolution du droit fondamental à la protection des données à caractère personnel ne sont pas pacifiques[1]. Alors que certains signalent la deuxième moitié des années

[1] Pour une vue d'ensemble sur la protection des données en Europe, voir le Manuel de droit européen en matière de protection des données (2014), élaboré par l'Agence des Droits Fondamentaux de l'Union Européenne et le Conseil de l'Europe, en association avec le greffe de la Cour Européenne des Droits de l'Homme.

soixante-dix comme l'étape fondatrice, d'autres situent l'embryon de cette discipline le 31 janvier 1968, avec la Recommandation 509 du Conseil de l'Europe[2].

Indépendamment de l'année de début, les premiers pas du droit à la protection des données personnelles se trouvent étroitement liés aux notions d'intimité ou de vie privée. De nombreux exemples démontrent ce lien :

- la *Privacy Act*, adoptée aux États-Unis d'Amérique en 1974, exprime la dépendance entre les deux figures[3] ;
- dans le continent européen, la protection des données personnelles se cristallise à travers la Convention 108 du Conseil de l'Europe[4] et l'art. 8 de la Convention Européenne des Droits de l'Homme (CEDH)[5] ;
- en ce qui concerne l'Union Européenne, une importante partie de ses États membres[6] ne consacre pas au niveau constitutionnel un droit fondamental à la protection des données personnelles, sinon que sa reconnaissance se produit, de manière générale, à partir du droit à l'intimité ou à la vie privée.

L'absence d'autonomie qui caractérise le droit à la protection des données personnelles n'équivaut pas à un manque d'action de la part des États. Elle reflète, entre autres choses, le stade de leur développement technique et économique. À l'époque de rédaction des premières Constitutions européennes post-Seconde Guerre mondiale, la protection des données personnelles n'y trouve pas de matérialisation en raison de la faible importance attachée à l'informatique. Ce panorama s'étend aux décennies suivantes malgré la, de plus en plus visible, prise de conscience au sein des États et des institutions européennes en ce qui concerne les dangers liés aux avancées technologiques[7].

---

[2] Recommandation 509 (1968) « *Droits de l'homme et réalisations scientifiques et technologiques modernes* », qui met en évidence les dangers que supposent pour la vie privée les dernières réalisations scientifiques et technologiques.

[3] Adoptée le 31 décembre 1974, la *Privacy Act* a pour objectif la sauvegarde de la vie privée des individus face à l'usage frauduleux de fichiers fédéraux. La relation entre vie privée et données personnelles est explicitement reconnue par le Congrès états-unien, qui, dans l'exposé de motifs de la loi, constate que la vie privée des individus est directement affectée par la collecte, maintenance, utilisation et diffusion d'informations personnelles par les agences fédérales.

[4] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en vigueur depuis le 1 octobre 1985.

[5] L'article 8 de la CEDH assure le respect de la vie privée et familiale. Cette prévision légale a été utilisée par la Cour Européenne des Droits de l'Homme (affaires *Amann c. Suisse*, *Rotaru c. Roumanie* et *S. et Marper c. Royaume-Uni*, entre autres), pour inclure dans son champ d'application la tutelle des données à caractère personnel.

[6] Dans une grande partie des textes constitutionnels européens, la protection des données personnelles n'est qu'un reflet du droit à la vie privée. C'est le cas, entre autres, de la France (où le droit à la vie privée trouve sa raison d'être dans l'art. 4 de la Déclaration des Droits de l'Homme et du Citoyen de 1789, bien que son expression littérale figure à l'art. 9 du Code Civil), la Belgique (art. 22 de la Constitution belge de 1831), l'Espagne (art. 18 de la Constitution espagnole de 1978) et le Luxembourg (art. 11.3 de la Constitution luxembourgeoise). Par contre, la Constitution grecque de 1975 dédie son art. 9 A à la protection des données personnelles et attribue à une autorité indépendante la garantie de son efficacité. La Constitution portugaise de 1976 va un peu plus loin en prévoyant, à son art. 35, le droit à la protection des données personnelles et en établissant une série de principes constitutionnels qui doivent être respectés par les pouvoirs publics lorsqu'une mesure dans ce domaine est envisagée.

[7] C'est à partir des années soixante-dix que les États de l'Europe occidentale commencent à dicter leurs premières lois sur la protection des données personnelles : l'Allemagne, en 1977, avec la Bundesdatenschutzgesetz, la France, en 1978, avec la Loi n° 8-17 relative à l'informatique, aux fichiers et aux libertés ou l'Autriche, aussi en 1978, avec la Datenschutzgesetz, entre autres. Parallèlement, en 1981 est adoptée au sein du Conseil de l'Europe

Ce n'est qu'à partir de la fin des années quatre-vingt-dix/début du XXIe siècle que la protection des données personnelles commence à se disjoindre de la vie privée : d'abord, avec 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 (ci-après « la Directive ») ; ensuite, avec la proclamation, en 2000, de la Charte des Droits Fondamentaux de l'Union Européenne (CDFUE), dont l'article 8 confirme l'indépendance de ce droit ; finalement, avec le Traité de Lisbonne, qui consacre la protection des données explicitement[8] et qui dote la CDFUE de force juridique contraignante[9]. L'époque où ces mesures sont adoptées n'a rien d'anodin : l'utilisation d'Internet se généralise de plus en plus tandis que les grandes entreprises qui domineront la sphère numérique dans les années qui suivent font leur apparition sur la toile.

Durant les dernières années, les institutions européennes ont rendu publique leur intention de renouveler l'encadrement légal de la protection des données avec l'approbation d'un règlement général qui abrogerait la Directive. Adopté par le Parlement Européen le 14 avril dernier conformément à l'art. 294.7/a) du Traité de Fonctionnement de l'Union Européenne, le nouveau 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 (Règlement général sur la protection des données)[10] (ci-après « le Règlement »)[11] a pour objectif de mettre à jour les normes relatives à la protection des données et d'accorder à l'espace européen une plus grande sécurité juridique[12], tout en préservant les garanties des individus. Toutefois, son application effective est différée jusqu'en mai 2018 (art. 99).

2. Encadrement de la problématique

La problématique qui oppose le traitement de données à caractère personnel à l'exercice d'autres droits fondamentaux n'est pas étrangère à la Directive. Le législateur européen a su,

la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, texte qui sera repris comme source d'inspiration pour rédiger la Directive 95/46/CE.

[8] Article 16.1 du Traité sur le Fonctionnement de l'Union Européenne, qui octroie à l'Union Européenne une base de compétence exclusive en la matière.

[9] Article 6.1 du Traité sur l'Union Européenne.

[10] JO L 119 du 4 avril 2016, pp. 1-88.

[11] Pour une vision critique sur les nouveautés apportées par le projet de Règlement, voir FALQUE-PIERROTIN, Isabelle, *Quelle protection européenne pour les données personnelles ?*, Fondation Robert Schuman, 2012. D'un point de vue économique, voir CAUCHOIS, Remi, « La protection des données personnelles en Europe et la compétitivité des entreprises européennes », en *Quelle protection des données personnelles en Europe ?* (Dir. Céline Castets-Renard), Larcier, 2015, pp. 157-164.

[12] La fragmentation juridique provoquée par la transposition de la Directive constitue, selon la Commission Européenne, l'une des raisons qui motivent un nouvel encadrement pour la protection des données. Cependant, cette affirmation se heurte au contenu des dispositions du Règlement. Trois aspects doivent être signalés : l'utilisation de concepts juridiques indéterminés, qui rend l'application du règlement extrêmement problématique (c'est le cas, notamment, de la notion de *suivi du comportement* présente à l'art. 3.2/b) du Règlement, relatif à son champ d'application territorial) ; les multiples délégations réalisées à la Commission et aux États membres afin de préciser certaines dispositions, qui intensifiera la complexité légale de cette matière ; la portée limitée du Règlement, qui n'affecte pas d'autres actes législatifs européens dans le domaine de la protection des données (dont la Directive 2002/58/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).

dans ce sens, identifier des situations conflictuelles et offrir des remèdes relativement efficaces[13].

Parmi les dispositions de la Directive qui manifestent la tension entre le droit à la protection des données personnelles et d'autres droits fondamentaux, la première qui mérite réflexion est l'art. 7/f). Cette prévision, reproduite dans l'art. 6.1/f) du Règlement, autorise le traitement de données personnelles si la satisfaction d'un intérêt légitime du responsable le rend nécessaire et à condition que les droits et les intérêts du titulaire des données ne prévalent pas. Comme la jurisprudence de la Cour de Justice de l'Union Européenne (CJUE) nous le montrera un peu plus tard, les droits fondamentaux sont susceptibles d'être insérés dans le concept d'intérêt légitime du responsable.

À l'art. 7/f) s'ajoute l'art. 8 de la Directive (art. 9 du Règlement), qui, après avoir établi une interdiction générale concernant le traitement de certaines catégories de données, prévoit des exceptions relatives notamment à la sauvegarde d'un intérêt vital du titulaire des données[14] (art. 8.2/c), repris dans l'art. 9.2/c) du Règlement). Cependant, c'est l'art. 9 de la Directive (art. 85 du Règlement) qui, de la manière la plus nette, reflète cette dispute en obligeant les États membres à prévoir des exemptions et des dérogations à certaines de ses dispositions afin de concilier le droit à la protection des données personnelles avec la liberté d'expression[15]. La dimension de la problématique n'est, toutefois, pas circonscrite aux seules dispositions de la Directive : d'autres droits fondamentaux non expressément visés par celle-ci sont susceptibles d'entrer en conflit avec le droit à la protection des données personnelles, ce qui rend nécessaire une analyse plus approfondie de la matière.

La conciliation entre droits fondamentaux impose des restrictions devant, en toute hypothèse, satisfaire certaines conditions d'ordre général contenues dans la CEDH et dans l'art. 52.1 de la CDFUE[16]. Les exigences qui doivent être observées sont au nombre de trois : la présence d'une raison légitimant les restrictions, une prévision légale expresse ainsi qu'un jugement de proportionnalité entre la mesure adoptée et l'objectif poursuivi qui devra, en tout cas, respecter le contenu essentiel du droit limité. Soulignons que de telles exigences sont requises non seulement lorsqu'un droit fondamental subit une restriction nécessaire pour préserver le droit à la protection des données personnelles, mais aussi lorsque la situation est inversée.

---

[13] Comme l'a déjà exprimé la Cour de Justice de l'Union Européenne, le législateur européen s'est efforcé de concilier les dispositions de la Directive avec d'autres droits fondamentaux susceptibles d'être affectés par son application (affaire C-101/01 « *Bodil Lindqvist* », §§ 84 et 90).

[14] L'art. 8.2/c) de la Directive ne constitue pas la seule base juridique qui légitime le traitement de données afin de sauvegarder un intérêt vital de son titulaire. Comme l'a déjà évoqué la CJUE, la protection de la vie et de l'intégrité physique peut excuser, sous la base de l'art. 7/f) de la Directive, des opérations de traitement de données appartenant à des tiers (affaire C-212/13 « *František Ryneš c. Úřad pro ochranu osobních údajů* », § 34). Signalons, en tout cas, que cet *obiter dicta* est, dans une certaine mesure, conditionné par les faits du cas d'espèce.

[15] Il s'agit, selon la CJUE, d'une véritable obligation juridique (affaire C-473/12 « *Institut professionnel des agents immobiliers c. Geoffrey Englebert et autres* », § 33), vision qui s'accommode à la doctrine de la Cour Européenne des Droits de l'Homme dans la mesure où elle impose aux États signataires de la CEDH l'adoption d'un cadre juridique approprié à l'exercice des droits y reconnus (voir, entre autres, l'arrêt de la Cour Européenne des Droits de l'Homme du 26 mars 1986 dans l'affaire *X et Y c. Pays-Bas*, § 23).

[16] Rappelons que, selon l'art. 52.3 de la CDFUE, le sens et la portée des droits contenus dans son texte seront les mêmes que ceux conférés par la CEDH, sans que cela ne puisse empêcher le droit de l'UE d'accorder une protection plus étendue.

Dans les pages qui suivent, nous analyserons l'application des critères de conciliation effectuée par la CJUE et la Cour Européenne des Droits de l'Homme (CeDH)[17]. Notre exposé se centrera sur le conflit entre le droit à la protection des données à caractère personnel et trois autres droits fondamentaux : la liberté d'expression et d'accès à l'information, le droit de propriété et la liberté d'entreprise.

II CONCILIATION AVEC D'AUTRES DROITS FONDAMENTAUX

1. Liberté d'expression et d'accès à l'information

1.1. Signification et contours jurisprudentiels

La liberté d'expression et d'accès à l'information constitue l'une des manifestations les plus emblématiques d'un État de Droit. Consacrée à l'art. 10 de la CEDH et à l'art. 11 de la CDFUE, elle représente une liberté individuelle fondamentale ainsi qu'un mécanisme indispensable pour contrôler l'action des autorités publiques. Le rôle joué par cette liberté est tel que les restrictions établies par le législateur arrivent même à être examinées avec une présomption d'inconstitutionnalité[18].

En ce qui concerne la liberté d'expression, la CeDH lui octroie une protection spécialement large en incluant une vaste étendue d'émanations sur la base des valeurs de pluralité, de tolérance et d'ouverture d'esprit, sans lesquelles une société ne pourrait être considérée comme démocratique[19]. Son exercice bénéficie, en outre, d'une tutelle plus accentuée dans le domaine politique[20]. Le fait que l'objectif poursuivi par celui qui l'exerce soit de nature lucrative[21] ou qu'Internet soit le moyen de diffusion utilisé[22] n'obstrue pas l'application de la CEDH. Par ailleurs, la CeDH a imposé aux États l'obligation de se doter d'un cadre législatif offrant des garanties suffisantes, tout en respectant l'exigence d'une prévision légale expresse et le devoir d'invoquer un besoin impérieux pour établir des restrictions jugées nécessaires[23].

La liberté d'accès à l'information a, à son tour, subi une évolution jurisprudentielle significative. De l'absence de l'obligation de faciliter la diffusion de l'information de la part de l'État[24], nous sommes passés à un véritable droit d'accès à l'information[25]. La liberté d'accès concerne le contenu de l'information ainsi que les moyens de transmission, dont Internet

[17] Nous utiliserons les abréviations CeDH et CEDH pour distinguer la Cour Européenne des Droits de l'Homme (CeDH) de la Convention Européenne des Droits de l'Homme (CEDH).
[18] Telle est la position assumée par la Cour Suprême des États-Unis de l'Amérique (arrêt du 30 juin 1976 dans l'affaire *Nebraska Press Assn. v. Stuart*, § V, entre autres). Pour une vision générale sur la liberté d'expression aux États-Unis, voir MUHLMANN, DECAUX & ZOLLER, *La liberté d'expression*, Dalloz, 2016, pp. 179-224.
[19] Arrêt de la CeDH du 16 décembre 2010 dans l'affaire *Aleksey Ovchinnikov c. Russie* (§ 39). L'idée est reprise par la CJUE dans l'affaire C-274/99 « *Bernard Connolly c. Commission* » (§ 39).
[20] Arrêt de la CeDH du 7 février 2012 dans l'affaire *Axel Springer AG c. Allemagne* (§ 90).
[21] Arrêt de la CeDH du 10 janvier 2013 dans l'affaire *Ashby Donald et autres c. France* (§ 34).
[22] Arrêt de la CeDH du 16 juin 2015 dans l'affaire *Delfi AS c. Estonie* (§ 110).
[23] Arrêt de la CeDH du 5 mai 2011 dans l'affaire *Comité de rédaction de Pravoye Delo et Shtekel c. Ukraine* (§§ 47-68). De la même façon s'est prononcée la CJUE (entre autres, affaire C-71/02, « *Herbert Karner Industrie-Auktionen GmbH c. Troostwijk GmbH* », § 50).
[24] Arrêt de la CeDH du 19 octobre 2005 dans l'affaire *Roche c. Royaume-Uni* (§ 172).
[25] Arrêt de la CeDH du 28 novembre 2013 dans l'affaire *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung c. Autriche* (§ 41).

assume une position centrale[26]. Cependant, des restrictions sont admissibles si une raison d'intérêt public les rend indispensables[27].

1.2. Problèmes posés par la Directive 95/46/CE

Comme nous l'avons déjà mentionné, la Directive prévoit, dans son article 9, l'obligation de la part des États membres d'introduire des exceptions à certaines de ses normes de manière à concilier la protection des données personnelles avec la liberté d'expression. Cette obligation pose, néanmoins, quelques problèmes de coordination et de nature interprétative.

Les difficultés interprétatives résultent du fait que les exceptions doivent répondre à des fins de *journalisme*[28] ou d'*expression artistique* ou *littéraire*. Cependant, les notions de *journalisme* et d'*expression artistique* ou *littéraire* ne sont pas définies par la Directive, bien que la CJUE ait déjà exprimé la nécessité d'une interprétation large[29]. Ce critère reste, toutefois, imprécis et donne aux États membres une marge d'appréciation non négligeable[30].

Outre son interprétation, la Directive laisse aux États membres la possibilité d'établir des exceptions à condition d'être nécessaires pour concilier la protection des données avec la liberté d'expression. Cela a pour conséquence la fragmentation de l'espace juridique européen, car chaque État détient le pouvoir d'établir les exceptions qu'il considère comme opportunes. Le Règlement aborde cette problématique dans son art. 85.1, en obligeant les États membres à prévoir des exemptions et des dérogations à certaines de ses dispositions afin de concilier la protection des données personnelles avec la liberté d'expression. Les concepts de *journalisme* et d'*expression artistique* et *littéraire* sont repris par le Règlement, auxquels s'ajoute celui d'*expression universitaire*, mais sans qu'aucune définition qui permette de les préciser ne soit offerte. En outre, le nouveau texte européen impose aux États membres l'obligation de notifier à la Commission les dispositions normatives adoptées en vertu de l'art. 85.1 (art. 85.3), ce qui aidera à mieux coordonner les règles nationales au fur et à mesure qu'elles seront adoptées.

1.3. Conciliation avec la protection des données personnelles

1.3.1. Liberté d'expression

La conciliation entre la liberté d'expression et la protection des données personnelles implique le besoin d'ériger certaines restrictions. Ces restrictions doivent, en tout cas, respecter les conditions imposées par les arts. 8.2 de la CEDH et 52.1 de la CDFUE. Par contre, si les limitations affectent la liberté d'expression, nous devrons faire appel à l'art. 10.2 de la CEDH ainsi qu'à la CDFUE.

En ce qui concerne la CJUE, l'établissement de restrictions à la protection des données au profit de la liberté d'expression a été examiné de manière partielle dans l'affaire C-73/07

[26] La fonction remplie par Internet est essentielle pour une société démocratique, car, selon la CeDH, il s'agit d'un moyen qui contribue grandement à la préservation et à l'accessibilité de l'actualité et des informations (arrêt du 10 mars 2009 dans l'affaire *Times Newspapers Ltd c. Royaume-Uni*, § 45).
[27] Arrêt de la CeDH du 27 novembre 2007 dans l'affaire *Timpul Info-Magazin et Anghel c. Moldova* (§ 31).
[28] Sur le concept de *journalisme*, voir VAN ENIS, Quentin, *La liberté de la presse à l'ère numérique*, Larcier, 2015, pp. 569 sqq.
[29] Affaire C-73/07 « *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy* », § 56.
[30] L'agence britannique de protection des données (ICO) a réalisé un important effort de clarification du concept de *journalisme* à travers son guide « *Data protection and journalism: a guide for the media*».

« *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy* ». Bien que les conditions pour bénéficier de la liberté d'expression soient interprétées d'une manière similaire à celle de la CeDH[31], la CJUE estime que le fait d'apprécier si une exception a été formulée *dans les limites du strict nécessaire* relève de la compétence des États membres, sans qu'aucune mention aux arts. 8.2 de la CEDH et 52.1 de la CDFUE ne soit effectuée. Par ailleurs, la CJUE juge que la seule divulgation au public d'informations, d'opinions ou d'idées constitue un motif suffisant pour qu'une activité bénéficie du titre de journalisme, sans analyser si la publication remplit une mission d'intérêt général qui puisse justifier des restrictions au droit à la protection des données personnelles.

Contrairement à la CJUE, la CeDH a développé une ample jurisprudence sous l'angle de l'art. 8 de la CEDH. L'absence d'une prévision spécifique sur la protection des données personnelles ne représente pas un obstacle pour la CeDH, qui offre une protection effective fondée sur le droit à la vie privée.

Le raisonnement de la CeDH s'inaugure avec la constatation d'une ingérence dans la vie privée. Cette constatation se produit d'une façon assez généreuse et rappelle la souplesse qui caractérise la notion de traitement de données consacrée à l'art. 2/b) de la Directive[32].

Ensuite, la CeDH examine si l'ingérence est admissible à la lumière de l'art. 8.2 de la CEDH. Le premier pas consiste à déterminer si l'exigence d'une prévision légale expresse a été remplie par le législateur, tant du point de vue formel que matériel[33]. Une fois que cela a été constaté, la CeDH analyse si l'ingérence est nécessaire à la protection de la liberté d'expression et conforme au principe de proportionnalité. Pour y parvenir, la CeDH s'appuie sur une série de critères développés par sa propre jurisprudence, l'élément central de son jugement étant le fait que l'information divulguée soit d'intérêt public ou susceptible d'ouvrir un débat intérêt général[34]. La liste des critères appliqués par la CeDH n'est, en aucun cas, exhaustive sinon indicative et en étroite dépendance des circonstances concrètes de chaque cas. Cela explique qu'aux lignes exposées dans l'arrêt *von Hannover c. Allemagne*[35] se soient ajoutées d'autres,

[31] En effet, la CJUE rappelle que la liberté d'expression s'applique non seulement aux entreprises de média, mais également à toute personne exerçant une activité de journalisme (§ 58), qu'une fin lucrative n'exclut *a priori* pas sa compatibilité avec ladite liberté (§ 59) et que le support utilisé pour s'exprimer ne constitue pas un critère déterminant pour apprécier s'il s'agit d'une activité journalistique (§ 60).

[32] Les situations qui, selon la CeDH, constituent une ingérence dans la vie privée se caractérisent par le fait d'être, à diverses occasions, subsumables dans le concept de traitement de données personnelles prévu à l'art. 2/b) de la Directive. Ainsi, la CeDH a considéré que la surveillance par GPS et le traitement des données obtenues par ce moyen constituaient une ingérence dans la vie privée (arrêt du 2 décembre 2010 dans l'affaire *Uzun c. Allemagne*). Cette affirmation est reprise pour les échantillons vocaux (arrêt du 25 septembre 2001 dans l'affaire *P.G. et J.H. c. Royaume-Uni*), la surveillance vidéo (arrêt du 17 octobre 2003 dans l'affaire *Perry c. Royaume-Uni*), les traitements à des fins journalistiques (arrêt du 9 octobre 2012 dans l'affaire *Alkaya c. Turquie*) ou les évaluations administratives (arrêt du 29 juillet 2014 dans l'affaire *L.H. c. Lettonie*).

[33] Pour que l'exigence d'une prévision légale expresse soit remplie, la CeDH impose deux conditions : que l'instrument utilisé revête un caractère normatif (élément formel) et que les conséquences découlant de son application soient suffisamment prévisibles (élément matériel), bien que l'usage de concepts juridiques indéterminés soit admissible (arrêt du 6 avril 2010 dans l'affaire *Flinkkilä et autres c. Finlande*, §§ 63-65).

[34] Qu'une publication soit d'intérêt public ou susceptible de promouvoir un débat d'intérêt général dépend des circonstances entourant chaque cas. Néanmoins, la CeDH a déjà reconnu l'existence d'un intérêt général lorsque la publication portait sur des affaires politiques, pénales ou même sportives et artistiques (affaire *Axel Springer AG c. Allemagne*, § 90).

[35] L'arrêt *von Hannover c. Allemagne* (7 février 2012) expose les critères généralement cités par la CeDH pour concilier la vie privée avec la liberté d'expression (§§ 109-113) : l'ouverture d'un débat public, le rôle joué par un

telles que la sévérité de la sanction imposée à l'éditeur d'un quotidien[36] ou l'objectivité et la bonne foi dans la présentation de l'information[37].

Notons que les solutions dispensées par la CeDH se caractérisent par son alignement avec l'esprit de la Directive et du Règlement. Ainsi, la liberté d'expression rencontre des limites lorsque l'ingérence a pour objet des données relatives à la santé[38] ou à une procédure judiciaire impliquant un mineur[39]. La CeDH a également appliqué de manière minutieuse le principe de qualité des données pour restreindre les traitements avec une finalité journalistique ou de diffusion publique aux données strictement nécessaires[40]. Par contre, lorsque la publication affecte des individus appartenant à la sphère politique, la protection accordée par l'art. 8 de la CEDH cède face à la liberté d'expression[41]. Le besoin que l'information s'insère dans un débat d'intérêt général est, toutefois, maintenu.

1.3.2. Accès à l'information

Les décisions de la CeDH portant sur le droit d'accès à l'information reprennent les critères signalés *supra*. À cet égard, les limitations imposées pour protéger les mineurs sont jugées opportunes[42] tandis que celles touchant des affaires relatives à la scène politique ou d'intérêt public ne sont pas qualifiées de la même façon[43].

La CJUE s'est également prononcée sur la validité de certaines restrictions imposées par le droit dérivé de l'UE à la protection des données personnelles. Les décisions de la CJUE suivent la structure de raisonnement de la CeDH : d'abord, en déterminant si le but poursuivi par la limitation est légitime et a été prévu par la loi ; ensuite, en examinant si l'application du principe de proportionnalité était adéquate. Ajoutons que tant la CDFUE que la CEDH sont utilisées par la CJUE comme canon de légalité des dispositions questionnées.

Selon les lignes tracées par la CJUE, les objectifs de transparence et de contrôle public de l'activité administrative à travers l'accès à l'information constituent des raisons d'intérêt général pour limiter le droit à la protection des données. Cependant, la balance s'équilibre à travers la minutie et la rigueur qui singularisent l'application du principe de proportionnalité.

---

individu dans la sphère publique, sa conduite préalable, le contenu, forme et conséquences de la publication ainsi que les circonstances dans lesquelles les données personnelles ont été traitées.

[36] Affaire *Axel Springer AG c. Allemagne*, § 95.

[37] Arrêt du 12 octobre 2010 dans l'affaire *Saaristo et autres c. Finlande* (§ 65).

[38] Dans les affaires *Armonienė c. Lituanie* et *Biriuk c. Lituanie* (25 novembre 2008), la CeDH a estimé que la divulgation de l'état de santé des requérants (qui étaient séropositifs) n'avait pas respecté les exigences de l'art. 8 de la CEDH (*cfr.* avec les arts. 8 de la Directive et 9 du Règlement).

[39] La publication de données relatives à la vie privée d'un mineur dans le contexte d'une procédure judiciaire a été jugée contraire à l'art. 8 de la CEDH (arrêt du 19 juin 2012 dans l'affaire *Kurier Zeitungsverlag und Druckerei GmbH c. Autriche*). Le Règlement n'est pas étranger à la problématique concernant le traitement de données appartenant à des mineurs et l'aborde dans plusieurs de ses articles (*cf.* arts. 6.1/f), 8, 12.1 et 57.1/b) du Règlement).

[40] Dans l'affaire *Alkaya c. Turquie*, la CeDH a considéré que la publication de l'adresse domiciliaire de la requérante par un quotidien national était excessive même si l'article dans lequel s'insérait l'information avait une finalité journalistique. Parallèlement, la CeDH a apprécié le caractère excessif d'une diffusion qui avait eu pour objet des données personnelles relatives à une activité de chauffeur datée de l'époque soviétique (arrêt du 3 septembre 2015 dans l'affaire *Sõro c. Estonie*).

[41] Affaires *Saaristo et autres c. Finlande* et *Flinkkilä et autres c. Finlande*, entre autres.

[42] Selon la CeDH, l'art. 6.1 de la CEDH autorise des mesures nationales qui ont pour effet de limiter l'accès à l'information de la part des journalistes (décision d'irrecevabilité « *Axel Springer AG c. Allemagne* », du 13 mars 2012).

[43] Arrêt du 14 avril 2009 dans l'affaire *Társaság a Szabadságjogokért c. Hongrie*, entre autres.

Cette précision analytique conduirait la CJUE à déclarer l'illégalité de certaines dispositions réputées excessives[44] ou à concilier des instruments de droit dérivé apparemment contradictoires afin d'obtenir le respect de l'art. 8 de la CEDH[45].

La doctrine de la CJUE a fait l'objet d'importants développements dans l'affaire C-131/12 « *Google Spain SL et Google inc. c. Agencia Española de Protección de Datos et Mario Costeja González* ». L'arrêt, extrêmement controversé, affirme, comme principe général, la prévalence du droit à la protection des données personnelles sur le droit d'accès à l'information de la part des internautes (§ 81)[46], tout en rejetant la possibilité que les moteurs de recherche puissent bénéficier de l'art. 9 de la Directive (§ 85)[47]. À la volonté d'établir une relation de hiérarchie entre droits fondamentaux s'ajoute un droit à l'oubli numérique qui, fondé sur les arts. 12/b) et 14/a) de la Directive, rend possibles la suppression des données personnelles ou l'opposition à leur traitement lorsque celui-ci s'effectue d'une manière contraire à la Directive (notamment en raison de leur caractère incomplet ou inexact) ou des raisons prépondérantes et légitimes tenant à la situation particulière du titulaire des données le justifie[48]. Compte tenu des difficultés liées à la conciliation entre les intérêts confrontés, il n'est pas surprenant que plusieurs guides sur l'application du droit à l'oubli[49] aient fait leur apparition.

Le droit à l'oubli soulève d'importantes incertitudes. Le fait de favoriser la protection des données personnelles au détriment de l'accès à l'information, uni à l'absence de critères précis pour concilier les deux droits, ont conduit certains à qualifier la décision de la CJUE de

[44] Dans son arrêt du 9 novembre 2010 (affaires jointes C-92/09 et C-93/09 « *Volker und Markus Schecke GbR et Hartmut Eifert c. Hessen* »), la CJUE a déclaré que la publication de certaines données personnelles visées par l'art. 44 *bis* du Règlement n° 1290/2005 et le Règlement n° 259/2008 ne gardait pas un rapport de proportionnalité avec l'objectif poursuivi (transparence et contrôle public de l'attribution d'aides provenant du FEAGA et du Feader) comme l'exigeait l'art. 52.1 de la CDFUE. Cette décision entraîne l'annulation de l'art. 44 *bis* du Règlement n° 1290/2005 et du Règlement n° 259/2008. Par contre, dans son arrêt du 20 mai 2003 (affaires jointes C-465/00, C-138/01 et C-139/01 « *Rechnungshof c. Österreichischer Rundfunk et autres* » et « *Christa Neukomm et Joseph Lauermann c. Österreichischer Rundfunk* »), la CJUE analyse une problématique similaire du point de vue de la CEDH, mais confie aux autorités judiciaires nationales le jugement de proportionnalité et la décision sur la légalité ou l'illégalité de la mesure discutée.

[45] Dans son arrêt du 29 juin 2010 (affaire C-28/08 P), la CJUE a conclu que l'accès aux documents en possession des institutions européennes (régi par le Règlement n° 1049/2001, relatif à l'accès du public aux documents du Parlement Européen, du Conseil et de la Commission) et contenant des données personnelles n'est possible que si le destinataire démontre la nécessité de les obtenir (condition prévue par l'art. 8/b) du Règlement n° 45/2001, 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), même si l'art. 6.1 du Règlement n° 1049/2011 ne prévoit pas l'obligation de justifier la demande d'accès.

[46] Cette approche se heurte à la position de la CeDH, qui considère que les droits contenus dans les arts. 8 et 10 de la CEDH méritent, comme règle générale, le même respect (affaire *von Hannover c. Allemagne*, § 106).

[47] Cette opinion contraste avec l'avis des Cours états-uniennes, qui reconnaissent la liberté d'expression des moteurs de recherche sous la base du Premier Amendement. Pour plus d'informations sur cette question, voir BRACHA, Oren, *The Folklore of Informationalism: The Case of Search Engine Speech*, Fordham Law Review, vol. 82, iss. 4, 2014, pp. 1629-1687.

[48] Pour une analyse approfondie concernant le droit à l'oubli, voir DE TERWANGNE, Cécile, « Droit à l'oubli, droit à l'effacement ou droit au déréférencement ? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique », en *Enjeux européens et mondiaux de la protection des données personnelles* (Dir. Alain Grosjean), Larcier, 2015, pp. 245-275.

[49] Deux guides sont de mention obligatoire : les lignes directrices du Groupe « Article 29» (Guidelines on the implementation of the Court of Justice of the European Union judgement on «*Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*» C-131/12, mises à jour par un rapport adopté le 16 décembre 2015) et le guide élaboré par un comité consultatif réuni sur demande de Google (The Advisory Council to Google on the Right to be Forgotten).

censure[50]. Malgré les dangers particuliers engendrés par Internet, la CJUE aurait pu soigner davantage l'expression de sa décision. Par ailleurs, que le droit à l'oubli ne soit pas applicable face aux propriétaires de sites web en raison de leur liberté d'expression[51] pose la question de savoir si leur droit ne devrait pas, dans certaines situations, reculer en faveur du titulaire des données. Le Règlement offre, dans son art. 17, la première réglementation formelle du droit à l'oubli au niveau européen et signale, comme exception, l'exercice du droit à la liberté d'expression (art. 17.3/a)). Cependant, aucun critère pour faciliter la conciliation n'est énoncé de manière expresse.

2. Droit de propriété

2.1. Protection nationale et internationale

Proclamé par l'art. 17 de la Déclaration Universelle des Droits de l'Homme, le droit de propriété constitue une manifestation primaire de la liberté individuelle, faisant partie intégrante des principes généraux du droit de l'UE, tel que souligné par la CJUE[52].

En tant que droit fondamental, la propriété profite d'une protection spécialement intense dans les ordres juridiques nationaux[53]. Cette protection se traduit également au niveau international dans l'art. 1 du Protocole Additionnel n° 1 à la CEDH (« le Protocole ») ainsi que dans l'art. 17 de la CDFUE.

Outre la propriété corporelle, tant le Protocole[54] que l'art. 17.2 de la CDFUE confèrent une attention particulière à la propriété intellectuelle. Le droit dérivé de l'UE occupe, dans ce domaine, une position de poids avec toute une série d'instruments normatifs[55].

2.2. Propriété intellectuelle, réseaux P2P et protection des données personnelles

2.2.1. Description de la problématique

L'environnement numérique entraîne de nouvelles menaces pour la propriété intellectuelle. L'évolution constante de l'industrie technologique implique le besoin d'une mise à jour permanente des normes réglant les différents droits de propriété intellectuelle. Parallèlement,

---

[50] La décision de la CJUE s'oppose aux précautions prises par la CeDH en ce qui concerne les pétitions d'effacement de données conservées par une autorité publique. Voir, dans ce sens, les arrêts de la CeDH dans les affaires *S. et Marper c. Royaume-Uni* (4 décembre 2008) et *Brunet c. France* (18 septembre 2014). Sur le premier, voir également BELLANOVA, Rocco & DE HERT, Paul, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », en *Culture & Conflits*, vol. 76, 2009, pp. 101-114.

[51] Affaire C-131/12 « *Google Spain SL et Google inc. c. Agencia Española de Protección de Datos et Mario Costeja González* », § 85.

[52] Arrêt de la CJUE du 13 décembre 1979 dans l'affaire C-44/79 « *Hauer c. Rheinland-Pfalz* » (§§ 13-16).

[53] En plus du contrôle de constitutionnalité *ex ante* et *ex post*, le droit de propriété est susceptible d'une protection renforcée à travers le recours d'amparo. Cependant, cette possibilité dépend, fondamentalement, de la portée attribuée à ce recours. Ainsi, tandis qu'en Espagne le droit de propriété (art. 33 de la Constitution espagnole) est soustrait du recours d'amparo car celui-ci est réservé aux droits compris entre les arts. 14 et 30 de la Charte espagnole (art. 161.1/b) en relation avec l'art. 53.2 de la Constitution espagnole), en Allemagne, la situation est l'inverse (art. 93.1/4b) en relation à l'art. 14 de la Constitution allemande).

[54] Malgré le silence de l'art. 1 du Protocole, la CeDH a déjà confirmé son application par rapport aux droits de propriété intellectuelle (arrêt du 11 janvier 2007 dans l'affaire *Anheuser-Busch inc. c. Portugal*, § 72).

[55] En ce qui concerne la propriété intellectuelle *stricto sensu*, au moins deux textes doivent être signalés : la Directive 2001/29/CE du Parlement Européen et du Conseil du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et la Directive 2004/48/CE du Parlement Européen et du Conseil du 29 avril 2004, relative au respect des droits de propriété intellectuelle.

elle donne lieu à des situations juridiques inédites qui imposent la concordance avec d'autres droits fondamentaux tels que la protection des données personnelles[56].

Parmi les innovations supposant un danger pour les droits de propriété intellectuelle, les réseaux P2P (*peer-to-peer*) occupent une place de premier plan. Ceux-ci permettent le partage de fichiers entre ordinateurs, augmentant ainsi les risques attachés à la circulation illicite de contenus protégés par un droit de propriété intellectuelle[57]. Afin de combattre ces pratiques de manière efficace, l'identification des contrefacteurs devient indispensable. Cependant, l'acquisition de ce genre de données s'oppose à l'obligation de confidentialité pesant sur les tiers qui les conservent.

L'obtention de données permettant l'identification d'éventuels contrefacteurs a soulevé deux questions fondamentales : celle concernant la base juridique légitimant la rupture de la confidentialité et celle portant sur les conditions qui doivent être respectées par les normes qui la permettent.

2.2.2. Base juridique légitimant l'intrusion

L'identification de ceux qui, à travers l'utilisation de réseaux P2P, portent atteinte à un droit de propriété intellectuelle requiert la communication de données personnelles de la part des fournisseurs d'accès à Internet. Toutefois, l'art. 5.1 de la Directive 2002/58/CE, relative à la protection des données dans le secteur des communications électroniques, impose la confidentialité des données qu'ils détiennent. Les États membres peuvent, malgré tout, formuler des exceptions (art. 15.1 de la Directive 2002/58/CE) lorsqu'elles sont nécessaires pour sauvegarder certains intérêts, parmi lesquels ne figure pas la protection civile de la propriété intellectuelle[58].

Le remède à cette lacune juridique semble être à l'art. 8 de la Directive 2004/48/CE, relative au respect des droits de propriété intellectuelle. Son paragraphe 1 prévoit l'obligation, pour les États membres, de garantir, dans le cadre d'une action relative à une atteinte à un droit de propriété intellectuelle, que les autorités judiciaires puissent ordonner au contrevenant ou à des tiers la communication de certaines informations. Néanmoins, l'art. 8.3/e) de la même directive affirme que ses paragraphes 1 et 2 s'appliqueront sans préjudice d'autres dispositions législatives et réglementaires régissant le traitement de données à caractère personnel. Cette clause serait employée par la CJUE dans l'affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* » pour exclure de l'art. 8.1 de la Directive 2004/48/CE la communication d'informations contenant des données personnelles[59]. Par contre, la CJUE souligne, dans la même affaire[60], que l'art. 15.1 de la Directive 2002/58/CE ne s'oppose pas à

[56] Pour une vision générale sur la relation entre droits fondamentaux et propriété intellectuelle, voir HELFER, Laurence R., *Human Rights and Intellectual Property: Conflict or Coexistence*, Minnesota Intellectual Property Review, vol. 5, n° 1, 2003, pp. 47-61.

[57] Toutefois, la seule existence ou utilisation d'applications P2P ne suppose pas, *per se*, une violation de la propriété intellectuelle, même si ce genre d'applications est, parfois, employé à des fins illégales.

[58] Selon l'art. 15.1 de la Directive 2002/58/CE, la confidentialité des données peut être limitée afin de sauvegarder la sécurité nationale, la défense et la sécurité publique ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques comme le prévoit l'art. 13.1 de la Directive 95/46/CE.

[59] Affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* », § 58.

[60] Affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* », §§ 53 et 54.

que les États membres prévoient l'obligation de divulguer des données personnelles dans le contexte d'une procédure civile pour la défense de la propriété intellectuelle. Il apparaît, par conséquent, qu'une telle faculté ne découle pas du droit de l'UE sinon que son exercice émerge *ex nihilo*.

La problématique que nous venons de décrire n'est pas nouvelle[61]. Elle affleure lorsqu'un certain fait (dans ce cas, le transfert d'information) est susceptible d'incarner plusieurs qualifications juridiques. En effet, l'art. 8 de la Directive 2004/48/CE constitue, d'un point de vue procédural, un moyen d'identifier le responsable de la lésion, mais implique, en même temps, un traitement de données personnelles[62] et une restriction aux arts. 7 de la CEDH et 8 de la CDFUE.

D'autre part, la solution apportée par la CJUE semble ne pas avoir exploré toutes les possibilités offertes par le droit de l'UE[63]. L'ambiguïté qui caractérise les règles européennes finit par accroître le sentiment d'insatisfaction.

Finalement, le fait que la communication de données personnelles ne soit pas obligatoire pour assurer la protection de la propriété intellectuelle a été questionné du point de vue de sa compatibilité avec l'art. 17 de la CDFUE[64]. La CJUE a, malgré tout, évité de répondre de manière expresse sur ce point en raison des possibles conséquences[65].

2.2.3. Validité de l'intrusion

Les traitements de données ayant pour objectif l'identification d'un infracteur de droits de propriété intellectuelle constituent une restriction au droit fondamental à la protection des données personnelles. Une telle restriction ne peut être admissible que si les conditions énumérées aux arts. 52.1 de la CDFUE et 8.2 de la CEDH sont satisfaites : prévision légale expresse, présence d'un objectif d'intérêt général et proportionnalité de la mesure[66].

---

[61] Voir la note n° 45.

[62] Cette qualification a été assumée par la CJUE dans les affaires C-275/06 « *Productores de Música de España c. Telefónica de España SAU* » (§ 45) et C-461/10 « *Bonnier Audio AB et autres c. Perfect Communication Sweden AB* » (§ 52).

[63] L'art. 13.1/g) de la Directive 95/46/CE, cité par la CJUE dans l'affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* » (§ 53), constitue une première option pour légitimer une restriction à la confidentialité des données imposée par la Directive 2002/58/CE. La portée générale de la première, unie à la fonction de complémentarité et précision de la deuxième (art. 1.2 de la Directive 2002/58/CE) favorise cette approche. Une deuxième option obligerait à considérer l'art. 8 de la Directive 2004/48/CE comme une source valable pour que la communication de données puisse être réalisée. Son articulation dans l'ordre juridique national s'accommoderait à l'art. 7/c) de la Directive 95/46/CE, qui habilite le traitement de données personnelles lorsque cela est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis. Cette solution s'ajusterait également à la logique des arts. 8.2 de la Directive 2004/48/CE et 8 de la Directive 2001/29/CE ainsi qu'à la pratique des États membres (confronter, dans ce sens, l'art. 8 de la Directive 2004/48/CE avec les §§ 20-23 et 54-57 de l'affaire C-461/10 « *Bonnier Audio AB et autres c. Perfect Communication Sweden AB* »).

[64] Affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* », §§ 61-70.

[65] Hormis une possible illégalité par omission, transformer la faculté de l'art. 15.1 de la Directive 2002/58/CE en une obligation supposerait une intrusion dans des domaines jugés extrêmement sensibles pour les États membres (sécurité nationale, défense…). Cependant, ne pas le faire blesserait l'esprit de l'art. 8 de la Directive 2001/29/CE.

[66] Le principe de proportionnalité, présent aux arts. 52.1 de la CDFUE et 8.2 de la CEDH, a été repris par le droit dérivé, notamment par l'art. 15.1 de la Directive 2002/58/CE, celui-ci imposant les principes de nécessité, proportionnalité et adéquation dans le contexte d'une société démocratique des mesures adoptées par les États membres (formulation similaire à celle employée par la CEDH). La nécessité en tant que condition de validité est également mentionnée par l'art. 13.1 de la Directive 95/46/CE.

La CJUE a déjà eu l'occasion d'analyser, d'une perspective tant abstraite que concrète, l'application des critères prévus dans les dispositions susmentionnées. Ainsi, dans l'affaire *Productores de Música de España c. Telefónica de España SAU*, la CJUE a exhorté les États membres à assurer, à travers leurs mesures législatives, un juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Cette recommandation s'étend aux autorités et juridictions nationales chargées d'interpréter et d'appliquer les mesures adoptées par les États membres[67]. Par contre, dans l'affaire *Bonnier Audio AB et autres c. Perfect Communication Sweden AB*, la CJUE a pu exercer un contrôle de légalité sur une disposition qui permettait la communication de l'identité d'une personne soupçonnée de contrefaçon. Selon la CJUE, la disposition réunissait les conditions suffisantes pour garantir un juste équilibre entre le droit à la protection des données et le droit de propriété intellectuelle. Dans ce sens, la CJUE a jugé que les conditions imposées par la norme en question (présence d'indices réels de contrefaçon, le fait que l'information demandée soit susceptible de faciliter l'enquête et que les raisons motivant l'ingérence soient d'un intérêt supérieur aux inconvénients occasionnés à son destinataire) respectaient les exigences résultant du principe de proportionnalité et parvenaient à un juste équilibre entre les intérêts opposés[68].

Pour conclure, nous signalerons une dernière précision en matière de mesures provisoires et conservatoires. Selon l'art. 9.1/a) de la Directive 2004/48/CE, les États membres doivent garantir que les autorités judiciaires puissent rendre des ordonnances de référé visant à prévenir toute atteinte imminente à un droit de propriété intellectuelle ou à empêcher des récidives. Cependant, dans les affaires C-70/10 « *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL* » et C-360/10 « *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA c. Netlog NV* », la CJUE a considéré qu'une injonction obligeant un fournisseur d'accès à Internet à une supervision illimitée de la totalité des communications électroniques afin de prévenir des infractions à la propriété intellectuelle ne garantissait pas l'équilibre entre le droit de propriété intellectuelle et la protection des données personnelles, en plus d'être contraire à l'art. 15.1 de la Directive 2000/31/CE, sur le commerce électronique[69].

2.3. Protection à travers l'art. 7/f) de la Directive 95/46/CE

À la différence de la propriété intellectuelle, la propriété corporelle trouve un moyen de protection *sui generis* dans l'art. 7/f) de la Directive. Cette disposition, dotée d'effet direct[70], habilite le traitement de données personnelles lorsque celui-ci est nécessaire à la réalisation

[67] Affaire C-275/06 « *Productores de Música de España c. Telefónica de España SAU* », § 68.
[68] Affaire C-461/10 « *Bonnier Audio AB et autres c. Perfect Communication Sweden AB* », §§ 58-60. En revanche, dans l'affaire C-580/13 « *Coty Germany GmbH c. Stadtsparkasse Magdeburg* », la CJUE a estimé qu'une disposition nationale autorisant, de manière illimitée, un établissement bancaire à exciper du secret bancaire pour refuser de fournir le nom et l'adresse d'un infracteur présumé de droits de propriété intellectuelle ne garantissait pas un juste équilibre entre la protection des données personnelles et le droit de propriété intellectuelle et devait, par conséquent, être déclarée contraire au droit de l'UE (§§ 36-41).
[69] Affaires C-70/10 « *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRLt* » (§§ 40 et 53) et C-360/10 « *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA* » (§§ 38 et 51).
[70] Affaires jointes C-468/10 et C-469/10 « *Asociación Nacional de Establecimientos Financieros y Federación de Comercio Electrónico y Marketing Directo c. Administración del Estado* », § 55.

d'un intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits fondamentaux du titulaire des données[71].

Selon la CJUE, l'art. 7/f) de la Directive impose la pondération des droits et intérêts opposés en fonction des circonstances considérées *in concreto*. Cette pondération devra, en tout cas, tenir compte de l'importance des droits de la personne concernée résultant des arts. 7 et 8 de la CDFUE[72].

La protection du droit de propriété *ex* art. 7/f) de la Directive n'a pas encore fait l'objet d'un examen approfondi par la CJUE. Toutefois, dans l'affaire C-212/13 « *František Ryneš c. Úřad pro ochranu osobních údajů* », la CJUE laisse la porte ouverte à cette voie en considérant que le traitement de données relatives à des tiers (dans le cas d'espèce, l'enregistrement d'images à travers un système de surveillance vidéo) s'avère justifié lorsque la finalité du traitement consiste à protéger les biens du responsable[73].

2.4. Nouveautés apportées par le Règlement

Les nouveautés introduites par le Règlement à l'égard des problématiques que nous avons signalées sont réduites, mais significatives.

En ce qui concerne l'identification de contrefacteurs faisant usage de réseaux P2P, le Règlement semble fournir une nouvelle solution à travers son art. 23 (homologue de l'art. 13 de la Directive). Cette disposition permet que le droit de l'Union Européenne ou le droit d'un État membre établissent des restrictions à certaines prévisions du Règlement lorsque celles-ci sont nécessaires pour garantir l'exécution de demandes de droit civil (art. 23.1/j)). De telles restrictions doivent constituer une mesure nécessaire et proportionnée dans une société démocratique ainsi que respecter l'essence des libertés et des droits fondamentaux. En outre, le Règlement ajoute, dans son art. 23.2, une série de dispositions que toute mesure législative adoptée conformément à l'art. 23.1 doit contenir, parmi lesquelles se trouvent la finalité du traitement, les catégories de données traitées ou la durée de leur conservation.

D'autre part, l'art. 6.1/f) du Règlement (art. 7/f) de la Directive) ajoute une nouvelle précision en exigeant une précaution additionnelle lorsque les données traitées appartiennent à un enfant.

3. Liberté d'entreprise

3.1. Contexte

La liberté d'entreprise (art. 16 de la CDFUE[74]) comprend, d'un point de vue classique, la faculté d'exercer une activité économique ainsi que l'interdiction, de la part de l'État, d'imposer des restrictions portant atteinte à son contenu essentiel. Son étendue se traduit également à

[71] Pour une vision plus étendue sur l'art. 7/f) de la Directive, voir l'Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la Directive 95/46/CE, élaboré par le Groupe de Travail « Article 29 ».

[72] Affaires jointes C-468/10 et C-469/10 « *Asociación Nacional de Establecimientos Financieros y Federación de Comercio Electrónico y Marketing Directo c. Administración del Estado* », § 40.

[73] Affaire C-212/13 «*František Ryneš c. Úřad pro ochranu osobních údajů*», § 34.

[74] Le silence de la CEDH par rapport à la liberté d'entreprise n'empêche pas que son existence soit déduite à partir d'autres droits fondamentaux comme la liberté d'association (art. 11 de la CEDH) ou le droit de propriété (art. 1 du Protocole).

l'intérieur de la propre entreprise, le pouvoir d'organisation et de direction de l'employeur étant l'une de ses manifestations les plus emblématiques.

L'usage généralisé d'appareils électroniques sur le lieu de travail a rendu nécessaire l'emploi de nouvelles mesures de contrôle sur les employés. Cette surveillance n'est, toutefois, pas exempte de difficultés dans la mesure où elle entraîne le traitement de données personnelles[75]. Par conséquent, la conciliation entre le pouvoir de direction de l'employeur et le droit fondamental à la protection des données relatives aux travailleurs s'impose[76].

Les prochaines lignes serviront à illustrer cette conciliation du point de vue normatif et jurisprudentiel. Les contributions du Règlement seront également reprises de manière à compléter notre analyse.

3.2. Légalité du traitement

3.2.1. Légitimation du traitement

L'employeur souhaitant traiter des données relatives à ses employés dans le cadre d'une opération de cybersurveillance doit s'assurer que le traitement réponde à l'une des situations prévues à l'art. 7 de la Directive (art. 6 du Règlement)[77]. Parmi celles qui semblent être susceptibles de légitimer le traitement se trouvent le consentement de la personne concernée (art. 7/a)), l'exécution d'un contrat auquel la personne concernée est partie (art. 7/b)) ou la réalisation d'un l'intérêt légitime du responsable (art. 7/f)). Le Groupe de Travail « Article 29 » (ci-après « le Groupe ») a manifesté des réticences à l'égard du consentement compte tenu du défaut d'équilibre qui caractérise, de manière générale, la relation de travail et des difficultés attachées à l'obtention d'un consentement pleinement libre de la part de l'employé. Cela a

[75] Les enjeux associés à la protection des données personnelles des travailleurs ont été exposés de manière précoce par le Conseil de l'Europe à travers sa Recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi (1989). L'Organisation Internationale du Travail a également contribué à ce sujet avec son Recueil de directives pratiques sur la protection des données personnelles des travailleurs (1997). Parallèlement, la CJUE s'est prononcée à plusieurs reprises sur l'application de la Directive aux traitements de données relatives à des travailleurs. Voir, dans ce sens, les arrêts dans les affaires jointes C-465/00, C-138/01 et C-139/01 « *Rechnungshof c. Österreichischer Rundfunk et autres* » et « *Neukomm et Lauermann c. Österreichischer Rundfunk*», C-342/12 «*Worten – Equipamentos para o Lar SA c. Autoridade para as Condições de Trabalho*» et C-683/13 «*Pharmacontinente – Saúde e Higiene SA et autres c. Autoridade para as Condições de Trabalho*».

[76] Les autorités nationales en matière de protection des données ont abordé cette problématique au moyen de différents rapports. C'est le cas, notamment, de l'ICO (Angleterre) avec son Code de pratiques en matière d'emploi (The employment practices code), la CPVP (Belgique) avec ses Recommandations visant à concilier les prérogatives de l'employeur avec la protection des données à caractère personnel des travailleurs ou de tiers lors de l'utilisation, de la surveillance et du contrôle des outils informatiques de communication électronique dans le cadre de la relation de travail ou l'AEPD (Espagne) avec son Guide sur la protection des données dans les relations de travail (Guía: La protección de datos en las relaciones laborales).

[77] Le fondement légitimant l'intrusion de l'employeur revêt une importance cruciale compte tenu des incidences que celle-là entraîne en matière criminelle, notamment en ce qui concerne le secret des communications. En outre, la surveillance des communications électroniques de l'employé peut occasionner des traitements de données sensibles (dans le sens des arts. 8 de la Directive et 9 du Règlement), ce qui impose des précautions additionnelles. Signalons, en tout cas, que tant la Directive (art. 8.2/b)) que le Règlement (art. 9.2/b)) prévoient la possibilité de réaliser des opérations de traitement de données sensibles lorsque le traitement est nécessaire pour respecter les obligations et les droits du responsable du traitement en matière de droit du travail et dans la mesure où il est autorisé par le droit de l'UE ou le droit national.

orienté le Groupe vers les situations prévues aux lettres b) et f) de l'art. 7 de la Directive au détriment du consentement, considéré comme une mesure de dernier ressort[78].

Les inquiétudes manifestées par le Groupe ont été prises en compte par le Règlement, qui, dans son art. 7, prévoit certaines garanties afin d'assurer la validité du consentement. Ainsi, lorsque le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, le Règlement oblige à ce que la demande de consentement soit présentée sous une forme qui la distingue clairement de ces autres questions, de manière compréhensible, aisément accessible et formulée en des termes clairs et simples (art. 7.2). En outre, et avec l'objectif de déterminer si le consentement a été donné librement, le Règlement impose l'obligation de vérifier si l'exécution d'un contrat est subordonnée au consentement au traitement de données qui n'est pas nécessaire à son exécution (art. 7.4).

3.2.2. Devoir d'information et principe de qualité

Indépendamment du motif légitimant le traitement, l'employeur devra remplir d'autres obligations imposées par la Directive.

Le devoir d'information présente, dans cette mesure, une importance capitale. Prévu à l'art. 10 de la Directive, il impose au responsable du traitement l'obligation de communiquer certaines informations au titulaire des données, telles que l'identité du responsable ou la finalité du traitement[79]. Cette communication résulte, en outre, indispensable pour garantir le respect du contenu essentiel du droit fondamental à la protection des données personnelles. Le Règlement reprend cette obligation dans son art. 13, amplifiant le catalogue d'informations à transmettre par le responsable du traitement.

Outre le devoir d'information, l'employeur est tenu de respecter scrupuleusement le principe de qualité (arts. 6 de la Directive et 5 du Règlement). Cela comporte, entre autres, une stricte observation des principes de finalité, nécessité et proportionnalité à l'égard des opérations de traitement.

3.2.3. Dispositions additionnelles contenues dans le Règlement

Contrairement à la Directive, le Règlement inclut une prévision (art. 88) permettant aux États membres d'adopter, par voie législative ou au moyen de conventions collectives et dans les limites marquées par ses dispositions, un régime spécifique pour le traitement de données en matière d'emploi. Ainsi, le Règlement s'aligne avec la pratique de certains États membres (dont la Belgique[80]) consistant à établir un régime juridique particulier en ce qui concerne les relations

[78] Avis 8/2001 sur le traitement de données à caractère personnel dans le contexte professionnel (adopté le 13 décembre), pp. 31-33.

[79] L'information contenue dans l'art. 10 de la Directive devrait être communiquée de sorte que l'employeur puisse prouver l'exécution de cette obligation. Son inclusion dans le contrat de travail ou la référence, par celui-ci, à la politique interne de l'entreprise en matière de cybersurveillance (à condition que celle-ci soit mise à disposition des employés sans aucune restriction) suffirait, en principe, pour l'attester.

[80] En Belgique, la cybersurveillance sur le lieu de travail est réglée par la Convention Collective de Travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau. Pour une vision complète sur la protection des données des travailleurs en Belgique, voir OMRANI, Feyrouze, « La vie privée du travailleur : questions choisies, regard critique », en *Droits de la personnalité*, Anthemis, 2013, pp. 99-148. D'un point de vue jurisprudentiel, voir LEONARD, Thierry & ROSIER, Karen, « La jurisprudence *Antigoon* face à la protection des

de travail. Les dispositions approuvées par les États membres devront, en tout cas, respecter les limites imposées par la dignité humaine et les intérêts légitimes et les droits fondamentaux des personnes concernées (art. 88.2).

3.3. Jurisprudence de la CeDH

L'absence de jurisprudence émanant de la CJUE en matière de cybersurveillance s'oppose à la consolidation de certaines lignes profilées par la CeDH.

Les décisions de la CeDH reposent sur une considération préliminaire d'ordre fondamental : le lieu de travail n'est, *a priori*, pas exclu de la protection garantie par l'art. 8 de la CEDH en raison d'une expectative d'intimité créée par le propre employeur, notamment lorsque la possibilité de cybersurveillance n'a pas été communiquée à l'employé[81]. La CeDH estime, dans cette mesure, que le devoir d'information de la part de l'employeur constitue une mesure indispensable pour assurer le respect de l'art. 8 de la CEDH.

Toutefois, dans l'affaire *Copland c. Royaume-Uni*, la CeDH a reconnu que l'art. 8 de la CEDH n'interdisait pas que l'employeur adopte des mesures de cybersurveillance lorsque cela s'avère nécessaire, dans une société démocratique, à la poursuite d'un but légitime[82].

Par contre, ce n'est qu'à l'occasion de l'affaire *Bărbulescu c. Roumanie*[83] que la CeDH a pu examiner si les critères employés par les autorités judiciaires nationales pour concilier le droit à la vie privée avec le pouvoir de cybersurveillance de l'employeur avaient pris suffisamment en compte les exigences imposées par l'art. 8 de la CEDH. Cependant, au lieu de développer sa jurisprudence, la CeDH se contente de reproduire l'avis des autorités nationales, même si cela soulève d'importantes controverses. Ainsi, la conviction, de la part de l'employeur, que les messages de courrier électronique possédaient un contenu purement professionnel ou le fait que l'employé n'ait pas été en mesure de signaler une raison valable pour justifier l'usage dudit courrier à des fins privées constituent, selon la CeDH, des arguments valides pour légitimer l'intrusion de l'employeur. La CeDH semble, néanmoins, oublier que l'employeur avait aussi accédé au courrier électronique privé de l'employé ou que le devoir d'information concernant les activités de cybersurveillance n'avait pas fait l'objet d'une preuve concluante. Cette situation est mise en évidence par le juge Pinto de Albuquerque qui, dans son opinion dissidente, rappelle que les employés n'abandonnent pas leur droit à la vie privée et à la protection des données chaque jour à la porte de leur employeur[84].

La décision dans l'affaire *Bărbulescu c. Roumanie* démontre que la jurisprudence européenne en matière de cybersurveillance est loin d'être consolidée. Soulignons, en tout cas, que l'évolution jurisprudentielle aux niveaux national et européen devra s'ajuster aux paramètres établis par la nouvelle réglementation sur la protection des données personnelles. Il se peut que l'art. 82 du Règlement anime les États membres en vue de trouver des solutions législatives qui

---

données : salvatrice ou dangereuse ? », en *Revue du Droit des Technologies de l'Information*, vol. 36, 2009, pp. 5-10.

[81] Voir, dans ce sens, les arrêts de la CeDH dans les affaires *Niemietz c. Allemagne* (16 décembre 1992, § 29), *Halford c. Royaume-Uni* (25 juin 1997, § 45) et *Peev c. Bulgarie* (26 juillet 2007, § 39).

[82] Arrêt de la CeDH du 3 avril 2007 dans l'affaire *Copland c. Royaume-Uni*, § 48.

[83] Arrêt de la CeDH du 12 janvier 2016 dans l'affaire *Bărbulescu c. Roumanie*.

[84] Opinion dissidente du juge Pinto de Albuquerque dans l'affaire *Bărbulescu c. Roumanie*, § 22.

concilient de manière plus incisive l'art. 8 de la CEDH avec le pouvoir de direction de l'employeur.

III CONCLUSIONS

1. Sur la jurisprudence de la CJUE et de la CeDH

Les lignes qui précèdent nous ont fourni une image des différentes problématiques associées à la conciliation entre le droit à la protection des données personnelles et d'autres droits fondamentaux. Il est donc temps d'exposer, sous forme de conclusion, quelques observations d'ordre général.

En ce qui concerne la relation entre protection des données et liberté d'expression, tant la CJUE que la CeDH confèrent une protection efficace au premier droit fondamental à travers l'application rigoureuse du principe de proportionnalité. Cependant, d'appréciables divergences écartent leurs positions : tandis que la CJUE priorise la protection des données personnelles face à l'accès à l'information, la CeDH pondère d'une manière beaucoup plus équilibrée les deux droits. Cette pondération est, à son tour, le fruit d'un long développement jurisprudentiel réalisé par la CeDH, dont les arrêts se révèlent techniquement plus élaborés que ceux de la CJUE.

La situation que nous venons de décrire contraste avec la conciliation effectuée entre le droit de propriété et le droit à la protection des données. La supériorité du deuxième n'est plus invoquée par la CJUE, qui semble préférer une formule basée sur un juste équilibre entre les droits confrontés et une stricte application du principe de proportionnalité. Toutefois, le fait que la CJUE ne se soit pas prononcée sur la compatibilité entre l'art. 17 de la CDFUE et l'absence du devoir de communiquer des données personnelles dans le cadre d'une procédure ayant pour objet l'infraction de droits de propriété intellectuelle affaiblit sa position initiale. D'autre part, la jurisprudence de la CJUE manque de maturité à l'égard de la propriété classique, ce qui empêche un examen plus exhaustif de la matière.

Finalement, la jurisprudence de la CeDH dans le domaine de la protection des données relatives aux travailleurs se caractérise par son inconsistance temporelle. Du protectionnisme face au pouvoir de surveillance de l'employeur, nous sommes passés à une marge de manœuvre plus étendue et moins respectueuse avec les principes découlant de la Directive et du Règlement. La jurisprudence de la CeDH est, en tout cas, loin d'être consolidée et susceptible de futures précisions qui aideront à tracer une ligne de raisonnement plus cohérente.

2. Sur les contributions du Règlement

Outre les nombreux ajustements techniques, le Règlement apporte certaines nouveautés en ce qui concerne la relation entre le droit à la protection des données personnelles et la liberté d'expression, l'encadrement du droit à l'oubli étant la plus emblématique. Les critères de conciliation restent, toutefois, dans les mains des États membres, qui devront établir des exceptions aux normes du Règlement de sorte qu'un équilibre entre les deux droits soit trouvé. Compte tenu de cette circonstance, nous pouvons affirmer que la jurisprudence nationale et européenne exercera un rôle essentiel dans les prochaines années.

Relativement au droit de propriété, le Règlement offre quelques nouveautés non négligeables, bien que plus modestes vu le développement de la jurisprudence de la CJUE. Quant à la cybersurveillance, le Règlement permet que les États membres élaborent des règles spécifiques en la matière, tout en imposant comme limites la dignité humaine et les droits fondamentaux. Les précisions concernant le consentement couronnent les grandes lignes établies par le texte européen.