

Les limites à l'utilisation des données personnelles

L'article suivant

La protection des données à caractère personnel et les médias

de Alexander Scheuer et Sebastian Schweda
est un extrait de la publication IRIS *plus* 2011-6
"Les limites à l'utilisation des données personnelles".
Cette publication est disponible sous forme imprimée
auprès de l'Observatoire européen de l'audiovisuel.
Pour plus d'informations et pour commander, veuillez cliquer sur :
Série IRIS *plus*
Publication IRIS *plus* 2011-6

Avant-propos

Fin septembre, Facebook a annoncé une extension prochaine du service qui permettra aux utilisateurs de constituer une « archive vivante » et d'offrir ainsi d'un seul clic tous les détails et les événements de leur vie privée à un nombre illimité d'« amis ». Qui aurait pu penser, il y a 20 ans, que ce projet serait perçu non comme la continuation de *1984* d'Orwell, mais comme une offre de service sérieuse et un modèle économique efficace ? Et qui aurait pu penser qu'un jour ce type de service nous amènerait à nous demander s'il existe encore une possibilité de contrôler les données à caractère personnel disponibles sur les systèmes électroniques et, le cas échéant, comment ? La réponse pourrait être la suivante : les initiateurs de la Convention européenne sur les droits de l'homme, tout au moins, croyaient en cette possibilité. En effet, certains sujets nous ramènent toujours vers des problèmes qui, en dépit de nouvelles apparences, sont connus de longue date. En ce qui concerne les données à caractère personnel, l'enjeu consiste à trouver un juste équilibre entre d'une part, le droit à la liberté d'information et d'expression, et d'autre part, la protection de la personnalité et de la vie privée. Or, la Convention a toujours été consciente de l'existence de ce champ de tension.

L'idée d'une archive vivante constituée de données personnelles est certes un cas extrême. Mais le fait est que dans les médias – notamment les médias audiovisuels – les risques de collision sont nombreux entre l'intérêt des médias à utiliser les données personnelles et l'intérêt des personnes concernées à protéger celles-ci. Il suffit d'évoquer, à cet égard, les reportages sur les personnalités publiques, les comptes rendus de procédures pénales ou les enquêtes des journalistes d'investigation. A l'ère de la communication bidirectionnelle, il existe également certaines situations où les utilisateurs de services de médias sont inquiets au sujet de la protection de leurs données personnelles. Les fournisseurs de services de médias ont un intérêt majeur à créer des profils de clients aussi précis que possible, car une parfaite connaissance des clients permet de leur proposer des offres adaptées sur mesure et de bénéficier ainsi d'un avantage concurrentiel.

La question visant à déterminer où se situe exactement la limite d'admissibilité dans l'usage des données personnelles n'a pas encore trouvé de réponse globale car, en définitive, cette délimitation dépend de l'évaluation au cas par cas des intérêts concurrents. En tout état de cause, on peut cependant tracer quelques lignes de démarcation à partir de la jurisprudence relative aux limitations de la liberté d'expression et d'information visant à préserver les données ou la vie privée. Mais il ne s'agit que de simples lignes dont le tracé est remis en cause en permanence, puisque chaque nouvelle forme d'utilisation des données et chaque nouvelle configuration des intérêts peuvent donner lieu à de nouveaux critères d'évaluation.

Les considérations pertinentes concernant l'étendue du droit à la liberté de l'information peuvent diverger sensiblement selon que, par exemple, l'intérêt d'un journaliste à mener des investigations pour un reportage télévisé se heurte au droit de la personne faisant l'objet du reportage à protéger sa vie privée, ou qu'un fournisseur de services de médias audiovisuels utilise à d'autres fins les données personnelles qui lui ont été communiquées librement par ses clients dans le cadre d'un abonnement à un service donné. Le législateur tente d'instaurer un minimum de clarté juridique avec des normes européennes et nationales, en dépit du flou inévitable propre à un système basé sur l'évaluation.

L'article de fond de ce numéro d'IRIS *plus* devrait permettre d'y voir plus clair dans les nombreux cas de figure d'utilisation des données personnelles faisant intervenir des droits fondamentaux concurrents. L'article distingue clairement deux types de situation : d'une part, les cas où les médias audiovisuels divulguent les données des personnes concernées, et d'autre part, les cas liés à la protection des données des utilisateurs de ces médias. L'article présente la législation en place au niveau de l'UE, tout en expliquant comment l'équilibre des intérêts a été maintenu, jusqu'à présent, entre les médias et les personnes concernées et entre les médias et leurs utilisateurs, à la lumière de plusieurs affaires posant des problématiques caractéristiques en la matière.

Etant donné que la protection des données personnelles pose des questions fondamentales liées au juste équilibre entre les droits de l'homme, le ZOOM de ce numéro d'IRIS *plus* est consacré à l'analyse des droits en question. Il expose comment la Cour européenne des droits de l'homme interprète l'article 10 de la Convention européenne des droits de l'homme (la Convention), qui joue un rôle clé pour les services de médias audiovisuels, ou comment la Cour de justice de l'Union européenne aborde la disposition équivalente, soit l'article 11, de la Charte des droits fondamentaux (la Charte) de l'UE. Puis il s'attache à examiner comment ces droits ont été formulés concrètement dans le droit secondaire. Tout en gardant cette approche binaire, l'article expose ensuite la problématique de la pondération des droits des personnes concernées au vu de l'article 8 de la Convention et des articles 7 et 8 de la Charte. L'article termine par un tour d'horizon du droit allemand en la matière pour illustrer les différentes façons de mettre en place des réglementations nationales à cet égard.

La partie « Reportages » s'inscrit entre les commentaires sur le droit européen du point de vue des différents cas de figure et les considérations concernant les droits fondamentaux conflictuels. Elle fait le point sur les développements des six derniers mois sur le thème de ce dossier, c'est-à-dire sur la définition des limites qu'il convient de poser à l'utilisation des données personnelles.

Strasbourg, octobre 2011

Susanne Nikoltchev
Coordinatrice IRIS

*Responsable du département Informations juridiques
Observatoire européen de l'audiovisuel*

La protection des données à caractère personnel et les médias

*Alexander Scheuer et Sebastian Schweda,
Institut du droit européen des médias (EMR), Sarrebruck/Bruxelles*

I. La liberté des médias et de l'information face aux droits de la personnalité : un conflit non résolu ?

« Profiter des données publiques, protéger les données privées ! » Cette phrase que l'on attribue au hacker et fondateur du Chaos Computer Club, Wau Holland, illustre un principe majeur de l'éthique des hackers¹. Il renvoie en même temps aux fondements de la législation européenne sur liberté des médias et de l'information d'une part et sur la protection des données d'autre part. Mais qu'est-ce qui est public et qu'est-ce qui est privé ? Concernant la forme des échanges d'information, le Web 2.0 démontre justement que les frontières entre communication publique et privée s'estompent de plus en plus. Les (*mass*) médias destinés au public montrent clairement que des données à caractère initialement privé peuvent très rapidement devenir publiques.

Le droit à la liberté d'information et à la liberté d'expression (notamment sous la forme particulière de la liberté de la presse et de la radiodiffusion) garantit que les médias puissent exercer leur mission, essentielle à la démocratie, qui consiste à rendre compte de la façon la plus exhaustive des événements d'intérêt public, en étant exposés le moins possible à l'ingérence de l'Etat ou de personnes privées². Ces règles permettent aux médias d'obtenir les informations nécessaires à leurs reportages dans le cadre des investigations menées et de les publier par la suite. L'exercice de ces droits trouve néanmoins ses limites lorsqu'il atteint un point d'interférence avec les droits d'autrui. Pour fournir des informations complètes à tous les utilisateurs des médias, il est presque toujours indispensable de collecter et de publier des données personnelles, c'est-à-dire à caractère personnel, sur les personnes faisant l'objet du compte rendu.

Il convient de faire une distinction fondamentale entre les activités de collecte (en tant qu'expression de la liberté passive de l'information) et de publication (liberté active de l'information),

1) Voir <http://www.ccc.de/hackerethics>

2) Voir à ce sujet ZOOM, section I.

car elles sont soumises à des réglementations différentes³. Le poids de la réglementation concernant ces deux activités fait écho au proverbe : « Une image en dit plus long que mille mots ». Dans le cadre d'un reportage photographique ou audiovisuel établissant qui a rencontré qui et à quel endroit, l'enregistrement et la publication d'une photographie ou d'un film constituent respectivement des traitements de données à caractère personnel conformément au droit en matière de protection des données. Du fait de ce traitement, les médias buttent presque inévitablement contre le droit des particuliers à la protection de la personnalité. Ce droit est, quant à lui, protégé par les normes des droits fondamentaux.

Le champ d'application des droits de la personnalité des personnes privées comprend, d'une part, la protection de la vie privée, c'est-à-dire d'un espace privé au sein duquel les informations doivent demeurer confidentielles. Cette zone est délimitée soit d'un point de vue spatial (le domicile, par exemple), soit, dans le cadre de la correspondance adressée à des personnes quantitativement identifiables, d'un point de vue théorique en fonction du contenu. D'autre part, le droit de la personnalité s'étend au-delà de la sphère purement privée et garantit également à chacun le droit intégral de pouvoir contrôler « l'image » de sa propre personne – y compris en dehors de la vie privée – diffusée à des tiers. Ce droit confère, au sens propre, « le droit à l'image », c'est-à-dire le droit de chacun de décider quelles photographies de sa propre personne doivent être accessibles. Mais une personne exerce également son droit de contrôle sur sa propre image en public lorsqu'elle se défend contre toute forme de représentation portant atteinte à son honneur ou à sa réputation. Enfin, le droit de la personnalité engendre également un « droit à l'autodétermination informationnelle⁴ ».

Il s'agit du droit d'une personne de disposer elle-même de toutes les informations la concernant, c'est-à-dire de toutes ses données à caractère personnel⁵. Ce qu'on appelle le droit général de la personnalité ne sert donc pas seulement à préserver la confidentialité de certaines informations, c'est-à-dire de les conserver dans la « sphère privée ». Ce droit vise également à garantir l'autonomie et l'autodétermination de chacun. Toute personne doit être en mesure de décider si des informations la concernant peuvent être transmises et, si oui, lesquelles. De cette façon, chacun peut déterminer quelle image de lui-même circulera dans la « sphère publique »⁶.

En 1974, le Comité des Ministres avait déjà demandé que toute personne concernée par un compte-rendu dans les médias ait le moyen de contrôler la représentation d'elle-même dans l'espace public. La résolution (74)26⁷ accorde à chacun un droit de rectification pour rétablir la vérité en cas de fausses allégations, et exige que cette rectification soit faite sans retard indu et, dans la

3) Voir plus en détail Egbert Dommering, « *Data, Information and Communication in 21st Century Europe: A Conceptual Framework* », dans : Thomas Kleist/Alexander Roßnagel/Alexander Scheuer (Ed.), *Europäisches und nationales Medienrecht im Dialog – Festschrift aus Anlass des 20-jährigen Bestehens des Instituts für Europäisches Medienrecht e.V. (EMR)*, volume 40 des cahiers de l'EMR, Baden-Baden 2010, p. 51 et s., 60, qui analyse tout d'abord cette différence entre traitement des données et traitement éditorial : « La première activité facilite l'archivage des informations, la seconde optimise la communication de ces informations au grand public comme une contribution au débat public. En conséquence, le traitement des données devrait être soumis aux dispositions régissant la protection des informations à caractère personnel, tandis que le traitement éditorial relève des dispositions concernant la libre circulation des informations. Alors que [par exemple] des archives de presse accessibles au public peuvent jouer un rôle de soutien dans le débat public, mais sans faire partie intégrante de ce débat, il est important, dans le cadre du droit de la presse et de la liberté d'expression, de prendre en considération le lien plus étroit existant entre ces archives et le débat. », avant de conclure : « Par conséquent, il est nécessaire de spécifier plus précisément les principes de la libre circulation de l'information et de la confidentialité des informations personnelles. »

4) La *Bundesverfassungsgericht* (Cour fédérale constitutionnelle allemande – BVerfG) a développé ce droit fondamental à partir du droit général de la personnalité dans un arrêt concernant le recensement de la population (BVerfGE 65, 1, 41 et s., et les références citées : <http://www.servat.unibe.ch/dfr/bv065001.html>).

5) Voir à propos de la protection des droits individuels ZOOM, section II.

6) Andreja Rihter, « *La protection de la vie privée et des données à caractère personnel sur Internet et les médias en ligne* », Rapport à la Commission de la culture, de la science et de l'éducation de l'Assemblée parlementaire du Conseil de l'Europe adopté à l'unanimité le 12 mai 2011, disponible sur : <http://www.assembly.coe.int/CommitteeDocs/2011/RihtervieprivéeF.pdf>, p. 8. Voir également Thomas Hoeren, *Persönlichkeitsrechte im Web 2.0*, dans : Thomas Kleist/Alexander Roßnagel/Alexander Scheuer (Ed.), op. cit. (note 3), p. 483 et s., 488 : « Dans une telle société de l'information, le droit de la personnalité est devenu un droit général d'autodétermination médiatique et informationnelle. »

7) Comité des Ministres, Résolution sur le droit de réponse – Situation de l'individu à l'égard de la presse. Les documents du Conseil de l'Europe sont disponibles sur : <https://wcd.coe.int/>

mesure du possible, avec la même visibilité que la publication initiale. Par ailleurs, toute personne devrait avoir la possibilité d'intervenir contre la publication de faits et d'opinions⁸ qui affectent sa vie privée ou portent atteinte à sa dignité, son honneur ou sa réputation.

Ce droit n'est limité que dans la mesure où la publication prévaut du fait d'un intérêt public légitime, ou est justifiée par le consentement – même implicite – de la personne concernée. Ces deux aspects de la protection des personnes concernées – droit à la vie privée et droit à la protection de la personnalité (tel que spécifié dans le paragraphe précédent, au sens strict d'un droit de contrôle de son image en public) peuvent, selon la résolution, servir à contrebalancer une liberté d'expression comprise au sens trop large. Les mesures de défense mentionnées ci-dessus contribuent de la sorte – parallèlement aux dispositions du droit de protection des données qui seront développées ultérieurement – à l'instauration d'un équilibre entre des droits fondamentaux conflictuels.

Les médias collectent et utilisent en particulier les données à caractère personnel dans leurs relations extérieures, car ils transmettent les données d'une personne concernée par un sujet médiatique aux utilisateurs de leurs services de médias. En outre, ils recueillent et utilisent des données à caractère personnel concernant ces mêmes utilisateurs⁹.

Dans la mesure où la personne concernée devient (involontairement) l'objet d'une activité journalistique, il convient, en premier lieu, de définir les limites des investigations et de déterminer la licéité d'un compte-rendu permettant l'identification des personnes concernées. La première partie du présent article (section II) s'attache à clarifier tout d'abord selon quelles règles du droit européen – droit des médias et / ou droit de la protection des données – il convient de répondre à ces questions. Ensuite, nous examinerons, à la lumière de plusieurs affaires emblématiques, comment est traitée au cas par cas la protection des personnes concernées en vertu de la jurisprudence des tribunaux européens et nationaux.

La protection des données des utilisateurs, en revanche, met en cause aussi bien les formes traditionnelles d'utilisation des médias, dans le cadre desquelles les données à caractère personnel des utilisateurs font l'objet d'un traitement, que les nouveaux médias « interactifs » : alors que la réception des émissions télévisées par voie terrestre, par satellite ou même par câble, ne requiert en principe aucun traitement des données, les services de télévision à péage et certains services complémentaires interactifs (tels que la participation à des jeux ou des sondages dans les émissions de « télévision interactive ») ne sont proposés que sous réserve d'un traitement des données personnelles des utilisateurs.

Les formes de médias qui sont apparues au cours de ces dernières années, en particulier, posent de nouveaux défis pour la protection des données des utilisateurs : les connexions bidirectionnelles – en particulier celles qui s'appuient sur le protocole Internet (basées sur l'IP) – offrent pour

8) Sur ce point, la résolution va plus loin que l'article 28 de la Directive 2010/13/EU (Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels (directive « Services de médias audiovisuels », version codifiée) JOUE du 15 avril 2010, L 95, p. 1 et s.). Le Journal officiel de l'UE et de la CE est disponible sur : <http://eur-lex.europa.eu>

9) Les données à caractère personnel font également l'objet d'un traitement interne dans le cadre de processus métiers internes en lien avec les informateurs et ceux qui « participent » aux médias. En ce qui concerne ces derniers, cela recouvre, entre autres, les journalistes, rédacteurs, animateurs, acteurs, invités des plateaux, techniciens et autres personnels employés ou mandatés par les sociétés de médias, par exemple, ceux dont le nom apparaît au générique d'une émission de télévision. Néanmoins, ces deux cas de figure n'ont pas leur place dans le présent article : la protection des informateurs et le secret éditorial ne relèvent pas, en principe, des règles de protection situées dans la zone de tension entre protection des données et liberté des médias. Au contraire, les concepts qui sous-tendent ces termes constituent des caractéristiques essentielles de la liberté des médias elle-même, qui doivent, du fait de leur orientation, protéger l'exercice de l'activité des médias, alors que la protection des personnes impliquées n'est qu'occasionnelle. En revanche, dans le cadre de la protection des données à caractère personnel des collaborateurs et / ou des employés des sociétés de médias, ces droits protecteurs n'interfèrent pas, normalement, avec la liberté des médias. Il convient, en général, de présumer le consentement car il est extrêmement rare qu'une personne participe sciemment et volontairement à un téléfilm sans consentir à la publication de son « nom réel », ou, en tous cas, d'un pseudonyme permettant de l'identifier (« nom d'artiste »).

la première fois aux utilisateurs un canal de retour permanent. L'intérêt majeur de ce dispositif réside dans la réutilisation des données aux fins de publicité comportementale. Sur la base des nouvelles possibilités techniques, des modèles novateurs d'entreprise se sont établis dans le Web « participatif » sous la forme des réseaux sociaux, tels que Facebook et les portails vidéo proposant des contenus générés par l'utilisateur (*user-generated content* - UGC).

Dans la deuxième partie de cet article (section III), nous aborderons dans un premier temps les conditions et les opportunités techniques puis nous analyserons les implications, en termes de protection des données, des différentes situations mises à jour. Pour cela, nous nous appuyerons sur le droit de protection des données en vigueur eu sein de l'UE et dans les Etats membres du Conseil de l'Europe. Pour finir, nous présenterons un aperçu des développements à venir et leurs répercussions sur les liens entre sphère publique et privée (section IV).

II. Les médias et la « protection des personnes concernées »

Les droits fondamentaux formant le socle du statut juridique des médias, des personnes concernées par les comptes rendus médiatiques et des utilisateurs des médias sont concrétisés par le droit secondaire de l'UE, qui contribue à résoudre les conflits entre la liberté d'expression et le droit de la personnalité.

Le Règlement (CE) n° 1049/2001 sur l'accès aux documents de l'UE¹⁰ garantit la liberté passive de l'information. Conformément à l'article 1 du règlement, il convient de garantir un accès aussi large que possible aux documents, ainsi qu'un exercice aussi aisé que possible de ce droit afin d'instaurer la transparence au niveau du fonctionnement des institutions de l'UE¹¹. Les conclusions de l'avocat général dans l'affaire *Schecke* exposent clairement que l'exigence de transparence dans l'administration publique est un motif légitime à la limitation du droit à la vie privée. A cet égard, l'objectif visant à développer l'ouverture dans une société démocratique doit être apprécié de façon fondamentalement positive. Cependant, la transparence « n'est pas nécessairement un bien absolu », et doit être mise en balance au cas par cas avec d'autres objectifs concurrents¹². Nous verrons par la suite qu'il en va de même avec les conflits d'intérêts entre d'une part, la protection des données et d'autre part, la liberté d'expression et des médias.

La Directive 95/46/CE¹³ comporte des dispositions relatives à la protection des données à caractère personnel. En principe, elle ne s'applique pas au traitement de données effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques telles que, par exemple, la correspondance privée (article 3, paragraphe 2, deuxième tiret). Dans l'affaire *Lindqvist*¹⁴, l'avocat général a limité la portée de cette restriction du champ d'application aux activités relevant de la vie strictement privée et familiale des personnes, ce qui n'englobe « manifestement pas » la diffusion de données à caractère personnel sur internet alors que ces données sont mises à la disposition d'un nombre illimité d'utilisateurs¹⁵.

10) Règlement n° (CE) 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, JOCE du 31 mai 2001, L 145, p. 43 et suivantes. Concernant la proposition de la Commission relative à l'adaptation du règlement (après l'entrée en vigueur du Traité de Lisbonne) et à son application en 2010, voir le rapport de la Commission du 12 août 2011, COM (2011) 492 final.

11) Concernant les droits des médias et des particuliers d'obtenir des informations de la part des organismes publics, voir Thorsten Ader/Max Schoenthal, *L'accès aux informations relatives aux activités de l'Etat, en particulier du point de vue des médias*, dans : Observatoire européen de l'audiovisuel (Ed.), IRIS *plus* 2005-2. Les articles de la série IRIS *plus* sont disponibles sur : http://www.obs.coe.int/oea_publ/iris/iris_plus/index.html

12) Conclusions de l'avocat général du 17 juin 2010, affaires jointes C-92/09 et C-93/09, *Schecke*, par. 94. Les conclusions de l'avocat général et les arrêts de la Cour de justice de l'Union européenne sont disponibles sur : <http://curia.europa.eu>

13) 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, JOCE du 23 novembre 1995, L 281, p. 31.

14) CJCE, arrêt du 6 novembre 2003, C-101/01, *Lindqvist*.

15) Conclusions de l'avocat général du 19 septembre 2002, C-101/01, *Lindqvist*.

1. Teneur des dispositions et interprétation de l'article 9 de la Directive 95/46/CE

En vertu de l'article 9 de la Directive 95/46/CE, les Etats membres peuvent prévoir des exemptions ou dérogations à l'application des dispositions de protection des données dans le cadre du traitement de données effectué « aux seules fins de journalisme ou d'expression artistique ou littéraire », mais

« dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression. »

Le considérant 37 de la Directive 95/46/CE souligne la nécessité d'aménager des exceptions, « notamment dans le domaine audiovisuel ». Par ailleurs, il énonce :

« (...) qu'il incombe donc aux États membres, aux fins de la pondération entre les droits fondamentaux, de prévoir les dérogations et limitations nécessaires en ce qui concerne les mesures générales relatives à la légalité du traitement des données, les mesures relatives au transfert des données vers des pays tiers ainsi que les compétences des autorités de contrôle (...) ; »

Toute exemption doit donc résulter d'une mise en balance des droits fondamentaux à la liberté d'expression et à la protection de la personnalité. La latitude conférée par l'article 9 de la Directive 95/46/CE quant à son interprétation devrait prendre fin là où le droit national n'assure plus un équilibre satisfaisant entre ces droits fondamentaux, du fait que le champ d'application des dispositions dérogatoires concernées est trop large ou trop étroit¹⁶.

Depuis la mise en œuvre de la Directive 95/46/CE, la Cour de justice de l'Union européenne (CJUE) n'a rendu que deux arrêts concernant l'interprétation de cette disposition :

Dans une procédure de décision préjudicielle concernant l'affaire *Lindqvist* déjà mentionnée, la question portait sur la diffusion de données à caractère personnel sur un site internet. La défenderesse dans l'affaire au principal, qui travaille comme catéchiste dans une paroisse, avait publié, sur une page destinée essentiellement aux paroissiens préparant leur confirmation, des informations au sujet de ses collègues de travail sans en avoir informé ces derniers, ni avoir recueilli leur consentement. Dans la procédure d'appel contre la décision qui condamnait la défenderesse à une amende, la cour d'appel nationale a saisi la CJCE, entre autres, de la question visant à savoir si la Directive 95/46/CE comportait des restrictions contraires à la liberté d'expression.

L'affaire *Satamedia*¹⁷ met en cause un service payant permettant aux utilisateurs de téléphones portables d'obtenir par SMS les données fiscales – publiées par ailleurs gratuitement par les services fiscaux finlandais – de personnes dont les revenus dépassent un certain seuil. Après une vaine tentative de la part des autorités finlandaises chargées de la protection des données d'obtenir la suspension du service de SMS, l'affaire est parvenue devant la Cour administrative suprême de Finlande, qui a saisi la CJUE, entre autres, pour savoir si les activités des deux sociétés pouvaient être qualifiées de traitement des données aux seules fins journalistiques.

a) Y a-t-il un traitement des données au sens visé par la directive ?

Dans les deux cas, il est pertinent d'examiner si l'utilisation des contenus en question constitue un traitement de données au sens visé par la Directive 95/46/CE. Il convient de noter que dans l'affaire *Satamedia*, la collecte et la publication de données sous forme imprimée, la diffusion des données sur CD-ROM, la préparation de la base de données et la mise à disposition par SMS ont été, selon les conclusions de l'avocat général (2008), suivies par la Cour, qualifiées de traitement de données à caractère personnel sans différenciation entre les divers procédés, alors que dans l'arrêt de l'affaire *Lindqvist*, en 2003, la Cour procédait à une analyse détaillée pour savoir si lors

16) Voir Conclusions de l'avocat général du 8 mai 2008, C-73/07, *Satamedia*, par. 100, concernant « l'exclusion quasi totale de la protection des données en cas de traitement des données à des fins de journalisme » dans le droit finlandais.

17) CJCE, arrêt du 16 décembre 2008, C-73/07, *Satamedia*.

du téléchargement des données sur un site, on était (déjà) en présence d'un traitement de données (sous forme de transfert vers un pays tiers). La CJCE a certes fait état, d'une façon générale, du stade de développement de l'internet au moment de la rédaction de la directive et du fait que celle-ci ne comportait pas de critères spécifiques concernant l'utilisation d'internet. Le fait qu'il s'agisse d'un traitement de données au sens visé par la directive a également été admis sans grande discussion à l'époque. La mise à disposition des informations sur le site internet implique « de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à internet¹⁸. »

b) *Comment identifier une activité journalistique (artistique, littéraire) ?*

Selon la CJUE, le support au moyen duquel sont transmises les informations n'est pas déterminant pour identifier une activité exercée exclusivement aux fins de journalisme. Que les données soient imprimées sur papier, diffusées sur les ondes ou transmises via un « support [...] électronique tel que l'internet » n'est pas déterminant pour en apprécier la finalité. Ainsi, par exemple, les blogs sur internet ne devraient pas, non plus, être exclus en principe du champ d'application de l'article 9 de la Directive 95/46/CE.

Lorsqu'un traitement de données est effectué à des fins *journalistiques*, conformément à l'article 9 de la Directive 95/46/CE, la CJUE raisonne en termes fonctionnels : non seulement les entreprises de médias pourraient se prévaloir d'un tel traitement, mais également toute personne qui mène une activité journalistique¹⁹. L'avocat général explique cela de la façon suivante :

« Autrefois, le journalisme se limitait à des médias (relativement) clairement identifiables en tant que tels, à savoir la presse, la radiodiffusion et la télévision. À l'heure actuelle, des moyens de communication modernes comme l'internet ou les services de télécommunications mobiles sont cependant également utilisés en vue de la communication d'informations sur des questions d'intérêt public tout comme à des fins purement privées. C'est pourquoi le type de communication d'informations constitue certes un élément important pour déterminer s'il y a des fins de journalisme, mais il convient de ne pas négliger le contenu. »

Mais quand peut-on dire que le critère matériel des « seules fins de journalisme » est rempli ? La Cour considère que cela recouvre des activités qui « ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées²⁰ ». Elle souligne d'une part, « l'importance que détient la liberté d'expression dans toute société démocratique, » et la nécessité d'interpréter les notions connexes, dont celle de journalisme, de manière large. D'autre part, afin de parvenir à une pondération pour rétablir l'équilibre avec le droit fondamental à la protection de la vie privée, les dérogations et limitations de la protection des données prévues doivent être limitées au strict nécessaire. Dans ce contexte, la CJUE rappelle également que l'avocat général avait souligné la nécessité de ne pas assimiler en bloc les termes de « fins de journalisme ou d'expression artistique ou littéraire » à la liberté d'expression, au risque de les vider de toute fonction propre au regard de cette notion²¹.

Pour « étoffer la notion de fins de journalisme », l'avocat général avait souligné le rôle de « chien de garde public » joué par une presse libre, tout en mentionnant l'obligation qui en découle

18) CJCE, *Lindqvist*, *op. cit.*, par. 26.

19) CJCE, arrêt du 16 décembre 2008, C-73/07, *Satamedia*, par. 59. Voir également CEDH, arrêt du 14 avril 2009, *Társarág a Szabadságjogokért (TASZ) contre Hongrie*, 37374/05, dans lequel la Cour reconnaît qu'un groupe d'intérêt peut jouer le rôle de « chien de garde social » en divulguant des informations. Les arrêts de la CEDH sont disponibles sur : <http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-fr>

20) CJCE, *Satamedia*, *op. cit.*, par. 61. Il faut néanmoins préciser que, conformément au considérant 47, la personne qui se borne à transmettre des contenus n'est généralement pas considérée comme responsable du traitement des données au sens visé à l'article. 2, paragraphe d de la Directive 95/46/CE (voir sur ce point ZOOM, section II. 2. a)). Le responsable du traitement de données est, le plus souvent, limité à « la personne dont émane le message ». Seule cette dernière pourrait donc invoquer, dans les circonstances exposées ici, les exceptions prévues par l'article 9 de la Directive 95/46/CE pour certains contenus.

21) Sauf mention contraire, les considérations suivantes sont extraites des Conclusions de l'avocat général, *Satamedia*, *op. cit.*, par. 56 et s., 66 et s., 73, 77 et s., 80 et s., 85.

« de communiquer des informations et des idées sur toutes les questions d'intérêt public ». Le traitement éditorial importe peu à cet égard ; la simple mise à disposition de données brutes peut contribuer au débat public. En cela, l'avocat général s'écarte quelque peu de la conception énoncée par les normes allemandes de mise en œuvre de l'article 9 de la Directive 95/46/CE, qui se basent sur l'existence d'un traitement de données « aux seules et propres fins journalistiques et éditoriales [des médias] ²². » D'après les commentaires de l'avocat général, on peut présumer que les informations communiquées présentent un intérêt public

« lorsqu'elles se rattachent à un débat public effectivement mené ou si elles concernent des questions qui, selon le droit national et les valeurs sociales, sont, selon leur nature, d'ordre public. »

Ce dernier groupe englobe les procédures judiciaires publiques, la transparence sur la politique, ainsi que les opinions et le comportement des dirigeants politiques. En revanche, l'intérêt public fait défaut quand il s'agit de détails de la vie privée d'une personne sans aucun lien avec une fonction publique « notamment lorsque, sur ce point, il y [a] une espérance légitime concernant le respect de la vie privée. » Cependant, il appartient aux médias, ne serait-ce qu'en partie, de créer l'intérêt public. Il n'appartient pas à l'Etat de prévoir leurs chances de réussite, car cela constituerait un premier pas vers la censure. Par conséquent, les autorités publiques ne peuvent présumer l'absence d'intérêt public que dans les cas évidents.

La jurisprudence de la CJUE ne traite pas plus en détail la question permettant de déterminer quand la finalité du traitement des données à caractère personnel peut être qualifiée d'*expression artistique* ou *littéraire*. Dans l'affaire *Lindqvist*, la Commission a effectivement reconnu les pages internet en cause comme une « création artistique et littéraire au sens de l'article 9 de [la] directive [95/46]²³. » Dans son arrêt, la CJUE n'est pas revenue sur cet argument. Par conséquent, il n'y a pas eu, jusqu'à présent, de définition juridique précise, en particulier en ce qui concerne les cas limites (par exemple, les films documentaires ou les formats d'info-divertissement). Néanmoins, dès lors qu'une offre représente davantage qu'une simple opinion, considérant qu'elle tombe dans le champ « médiatique » défini par les trois domaines « d'activité journalistique », « d'expression artistique » et « d'expression littéraire », une restriction supplémentaire à l'alternative réelle est inutile puisque les conséquences juridiques sont identiques.

c) *Quand le traitement des données est-il opéré exclusivement aux fins énoncées ?*

L'exigence d'un traitement de données à des fins *exclusivement* journalistiques ne signifie pas que le traitement doive « avoir pour objet la communication directe d'informations ». Les recherches nécessaires menées en amont de la publication relèvent également de cette finalité. La question de savoir si, au cas par cas, un traitement de données est destiné *uniquement* à des fins journalistiques doit faire l'objet, selon l'avocat général, d'une appréciation qualitative, ce qui devrait permettre de dégager la finalité à partir de circonstances objectives. Les visées subjectives du responsable de traitement ne sont pas pertinentes.

A cet égard, la CJUE estime que l'existence d'un but lucratif n'exclut pas, non plus, la possibilité qu'une publication soit réalisée aux « seules fins de journalisme » : au contraire, « un certain succès commercial peut même constituer la condition *sine qua non* de la subsistance d'un journalisme professionnel²⁴ » .

22) Voir article 41, par.1 de la *Bundesdatenschutzgesetz* (loi fédérale sur la protection des données - BDSG). Toutefois, le *Bundesgerichtshof* (Cour fédérale de justice - BGH) considère ces conditions comme réunies dès lors que la publication est destinée à un nombre indéfini de personnes et qu'il y a une volonté d'exprimer une opinion. Voir Sebastian Schweda, IRIS 2011-5/12, et Anne Yliniva-Hoffmann, IRIS 2010-2/9. Tous les articles de la lettre d'information IRIS sont disponibles sur : <http://merlin.obs.coe.int> . Ainsi, même en droit allemand, la question de savoir qui peut invoquer le « privilège des médias » ne dépend pas de la forme de la publication, mais exclusivement de l'activité elle-même – qui doit être de nature journalistique. Les portails internet peuvent donc également revendiquer cette protection.

23) CJUE, *Lindqvist*, *op. cit.*, par. 33.

24) CJUE, *Satamedia*, *op. cit.*, par. 82. D'après ce qui précède, on ne peut renoncer à postuler des « seules fins journalistiques » que dans le cas où il existe des intérêts commerciaux liés à une publication qui ne servent pas à diffuser des informations ou des idées sur des questions d'intérêt public (par ex. la diffusion de publicité par les médias, voir Conclusions, par. 84).

d) Autres exemples tirés de la pratique des Etats membres

La question de savoir si des données à caractère personnel peuvent être traitées à des fins journalistiques se pose également en lien avec les sites de classement sur internet. Si, par exemple, le compte-rendu d'un film juge la « performance » des acteurs sur une page de critique cinématographique, cela entraînera nécessairement la publication de données à caractère personnel. Dans deux des nombreuses décisions rendues par les juridictions nationales, qui portent chacune sur la recevabilité d'une plateforme internet de notation des performances professionnelles des enseignants (« spickmich.de » et « note2be.com »), le *Bundesgerichtshof* (Cour fédérale de justice allemande - BGH)²⁵ et le Tribunal de Grande Instance de Paris (TGI)²⁶ sont parvenus à des conclusions divergentes : en dépit de leur caractère fondamentalement similaire, le modèle économique de « spickmich.de » a été jugé légal, tandis que « note2be.com » était déclaré illégal.

Les deux juridictions ont tout d'abord analysé le rapport entre la liberté d'expression et le droit à l'autodétermination informationnelle (en tant que droit de la personnalité des enseignants). Selon le BGH, aucun intérêt légitime de la requérante ne s'oppose à l'enregistrement, car les évaluations contestées se basent uniquement sur ses activités professionnelles. Le BGH souligne que la participation à un forum public d'opinion devrait être, en principe, autorisée même si des données personnelles y sont transmises. Dans le cas contraire, cela signifierait que la liberté d'expression et d'information « serait limitée à des déclarations dénuées de tous contenus protégés en leur qualité de données. » Or, on ne peut, dans ce cadre, compter sur le consentement de la personne concernée, d'autant moins si les commentaires sont négatifs, de sorte que toute évaluation deviendrait ainsi « quasiment impossible. » Le BGH considère que la norme allemande de mise en œuvre de l'article 9 de la Directive 95/46/CE n'est pas pertinente, en l'espèce, puisqu'il ne saurait être question de traitement de données « aux seules et propres fins journalistiques et éditoriales », conformément à la norme, que si « l'effet formateur sur l'opinion publique constitue un élément caractéristique de l'offre et ne se limite pas à un rôle accessoire purement superficiel. » Il s'avère que l'offre de l'opérateur de la plateforme en cause ne correspond pas à ce critère²⁷.

Le TGI ne s'est nullement préoccupé de l'article 9 de la Directive 95/46/CE. Au lieu de cela, il met en balance la liberté d'expression et d'information et l'intégrité de l'activité d'enseignement. Considérant que la publication des notes des enseignants avec mention nominative est propre à perturber cette intégrité, le TGI a rendu une injonction d'interdiction.

e) Les prochains développements de la disposition dérogatoire

Dans ses propositions de réforme du droit européen en matière de protection des données²⁸, la Commission n'a pas statué sur l'avenir de la disposition de l'article 9 la Directive 95/46/CE. Cependant, le Parlement européen a souligné dans sa résolution²⁹ l'importance de cette disposition en invitant à cet égard la Commission à tout mettre en œuvre « pour évaluer la nécessité d'étendre ces dérogations [...] afin de protéger la liberté de la presse. » Dans le contexte du développement technologique, le Parlement souhaite assurer le maintien d'un niveau élevé de protection des

25) BGH, arrêt du 23 juin 2009, VI ZR 196/08, disponible sur : <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=2f87ec5b9cc2c0d5e8fe748b700898ea&nr=48601&pos=0&anz=1>

26) TGI, ordonnance de référé du 3 mars 2008, n° RG : 08/51650, disponible sur : <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/tgi-par20080303.pdf>. L'ordonnance a été confirmée par un arrêt de la cour d'appel de Paris du 25 juin 2008, n° RG : 08/04727, <http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/IMG/pdf/ca-par20080625.pdf>

27) BGH, *op. cit.* (note 25), par. 21. Fondamentalement, le BGH considère que la « presse électronique » relève également du champ de protection de la liberté d'expression ; voir BGH, *op. cit.* (note 25), par. 20.

28) Communication du 4 novembre 2010 de la Commission au Parlement européen, au Comité économique et social européen et au Comité des régions – « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », COM(2010) 609 final.

29) Résolution du Parlement européen du 6 juillet 2011 sur une approche globale de la protection des données à caractère personnel dans l'Union européenne, P7_TA(2011)0323, disponible sur : <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=FR&ring=A7-2011-0244>

données, tout en s'assurant « qu'un juste équilibre entre le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information » est garanti.

Le responsable européen de la protection des données (*European data protection supervisor* – EDPS) reconnaît les différences culturelles existant entre les divers Etats membres en matière de liberté d'expression et suggère d'exclure des travaux d'harmonisation le champ des exceptions règlementé par l'article 9 de la Directive 95/46/CE - à l'exception de la modernisation de la réglementation à la lumière des développements actuels sur l'internet³⁰. L'Union européenne de radiodiffusion (UER) s'exprime encore plus clairement en faveur du maintien³¹ et du renforcement des exonérations. Concernant la proposition de la Commission d'instaurer un « droit à l'oubli », l'UER appelle à la prudence : le droit de toute personne à garder le contrôle des informations la concernant doit être clairement distingué de la possibilité de disparaître des contenus médiatiques. La tâche des médias d'assurer une telle couverture doit être préservée pour le bénéfice social global³².

2. Conciliation des intérêts respectifs des médias et des personnes concernées

Le conflit entre la liberté des médias et la protection de la personnalité se cristallise essentiellement à deux niveaux (voir I) : d'une part, il porte sur la légitimité du traitement des données à caractère personnel en amont d'une éventuelle publication, c'est-à-dire au niveau des investigations, au terme desquelles il sera décidé si « le sujet » est approprié et pertinent pour un compte-rendu médiatique, et si oui, dans quelle mesure ; d'autre part, il concerne le moment où l'information est effectivement mise à la disposition du public. Les comptes rendus sur des procédures pénales présentant un intérêt public, sur la vie privée et l'intimité de personnes qui se trouvent au centre de l'intérêt public (responsables politiques, célébrités), et sur des questions pour lesquelles les informations ont été obtenues illégalement, peuvent transgresser profondément les droits des personnes concernées.

a) « La protection des données éditoriales » : collecte et utilisation des données à caractère personnel « au sein de la rédaction »

Pour établir un juste équilibre, les droits de protection individuels doivent être conçus de sorte à laisser suffisamment d'espace aux médias pour leurs investigations. Ces derniers doivent avoir au moins le droit d'enquêter sur toutes les données à caractère personnel qu'ils sont susceptibles de pouvoir publier ultérieurement, le cas échéant.

En principe, les journalistes bénéficient donc d'un droit d'investigation étendu, et sont même investis d'une obligation de procéder à des recherches élargies pour assurer une couverture équilibrée. Des injonctions d'interdiction préventives de la part des personnes concernées auraient pour effet d'entraver de telles recherches. Par exemple, lors de l'utilisation de « caméras cachées » pour détecter des activités potentiellement illégales ou répréhensibles de la personne concernée, il est nécessaire d'enquêter soigneusement au préalable sur les faits pour pouvoir juger s'il est pertinent de couvrir ce sujet. C'est justement lorsque l'utilisation licite des informations apparaît envisageable que les mesures préventives de protection juridiques contre les investigations ne doivent pas être

30) Avis du contrôleur européen de la protection des données sur la communication de la Commission — « Une approche globale de la protection des données à caractère personnel dans l'Union européenne » JOUE du 22 juin 2011, C 181, p. 1 et s.

31) De même que l'avis de la chaîne allemande Zweites Deutsches Fernsehen (ZDF), qui s'appuie en particulier sur l'interprétation large de la règle des exceptions par la CJUE dans l'affaire *Satamedia* (op. cit.) ; http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/zdf_de.pdf

32) UER, Comments concerning the consultation on the Commission's Communication – « A comprehensive approach on personal data protection in the European Union », 14 janvier 2011, http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/ebu_en.pdf

garanties³³. Ce n'est que lorsqu'il apparaît clairement, au vu des méthodes d'investigation, que le compte-rendu sera manifestement illégal, et que les personnes concernées subiront de ce fait un préjudice irréparable, qu'il doit être possible d'interdire le travail d'investigation³⁴. D'importantes restrictions du travail d'investigation existent également dans le cadre des procédures juridiques. Ceci s'applique en particulier à l'enregistrement vidéo des audiences judiciaires³⁵.

Inversement, il convient également de considérer que des données dont la collecte n'est pas autorisée ne peuvent être publiées que dans des cas exceptionnels, nonobstant la liberté d'expression. Le respect des lois par la personne concernée peut, à cet égard, se révéler comme un critère de démarcation important³⁶.

b) *Conciliation entre liberté des médias et protection de la personnalité au niveau de la publication : comptes rendus permettant l'identification*

aa) La couverture actuelle des procédures administratives et judiciaires, notamment criminelles

La Cour européenne des droits de l'homme (CEDH) reconnaît aux médias le droit de faire des comptes rendus sur les procédures judiciaires pour informer le public³⁷, et se réfère également à la Recommandation du Comité des Ministres Rec (2003)13³⁸. Toutefois, la Cour souligne qu'il ne faut pas perdre de vue la norme de diligence journalistique. L'exercice de la liberté d'expression comporte des devoirs et des responsabilités, qui s'appliquent également à la presse³⁹. Des déclarations peuvent être condamnables en particulier lorsqu'elles compromettent les chances de la personne concernée d'avoir un procès équitable conformément à l'article 6, paragraphe 1 de la Convention européenne de sauvegarde des droits de l'homme (la Convention)⁴⁰.

Concernant le compte-rendu audiovisuel, la « protection de la réputation ou des droits d'autrui » pourrait justifier une ingérence dans l'exercice de la liberté d'expression⁴¹. Dans le cas d'*Österreichischer Rundfunk*⁴² (radiodiffuseur public autrichien), la CEDH a déclaré une injonction d'interdiction à l'encontre d'ORF contraire au droit à la liberté d'expression (article 10 de la Convention). Cette injonction interdisait à l'ORF de diffuser la photo d'un néo-nazi dans le cadre d'un compte-rendu sur la condamnation de ce dernier, en considération du fait qu'il pouvait soit purger sa peine, soit bénéficier d'une libération conditionnelle. La CEDH a apprécié la recevabilité d'une restriction de la liberté d'expression uniquement en regard des critères suivants : le niveau de notoriété de l'intéressé, le temps écoulé depuis sa condamnation et sa libération, la nature du délit, le lien entre le contenu du compte-rendu et la photo présentée, ainsi que l'exhaustivité et l'exactitude du texte d'accompagnement. La CEDH a souligné les différences existant avec une autre affaire mettant en cause les mêmes parties⁴³, qu'elle avait jugée irrecevable. L'ORF avait, dans le cadre d'un compte-rendu sur une série de lettres piégées, montré la photo d'un présumé suspect,

33) Cf. l'arrêt du 8 mars 2010 de l'*Oberlandesgericht* de Düsseldorf, 20 U 188/09, disponible sur : http://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2010/I_20_U_188_09urteil20100308.html, dans le cas de réalisation d'enregistrements vidéo en caméra cachée dans un cabinet médical. Le tribunal a jugé qu'une utilisation dans le cadre d'un bref compte-rendu pouvait être licite dans la mesure où les personnes filmées ne peuvent pas être identifiées. Concernant la situation au regard du droit français, voir *Amélie Blocman*, enregistrements en caméra cachée, IRIS 2009-10/12.

34) Cf. la décision du 27 mai 2010 de l'*Oberlandesgericht* (tribunal régional supérieur) de Coblenz, 4 W 170/10. Dans cette affaire, un médecin avait fait l'objet d'une enquête après une série de décès suspects parmi ses patients. Après la clôture de l'enquête, l'interview de deux de ses patients avait été programmée dans le cadre d'un reportage télévisé. Le médecin avait obtenu une ordonnance de référé contre toute mention de son nom dans le cadre du reportage.

35) Voir également sur ce point CEDH, arrêt du 24 avril 2001, *B. et P. contre Royaume-Uni*, n° 36337/97 et 35974/97.

36) Voir sur ce point l'arrêt exposé ci-après (section II. 2. c) de la BVerfG.

37) CEDH, arrêt du 7 juin 2007, *Dupuis et autres contre France*, n° 1914/02, par. 42.

38) Recommandation du 10 juillet 2003 du Comité des Ministres aux Etats membres sur la diffusion d'informations par les médias en relation avec les procédures pénales ; voir à ce sujet ZOOM, section I. 2.

39) CEDH, arrêt du 10 février 2009, *Eerikäinen et autres contre Finlande*, n° 3514/02, par. 60 ; arrêt du 6 avril 2010, *Flinkkilä et autres contre Finlande*, n° 25576/04, par. 77.

40) CEDH, arrêt du 29 août 1997, *Worm contre Autriche*, n° 83/1996/702/894.

41) CEDH, arrêt du 16 avril 2009, *Egeland et Hanseid contre Norvège*, n° 34438/04, par. 59.

42) CEDH, arrêt du 7 mars 2007, *Österreichischer Rundfunk contre Autriche*, n° 35841/02.

43) CEDH, arrêt du 25 mai 2004, *Österreichischer Rundfunk contre Autriche*, n° 57597/00.

mais sans faire mention de l'acquiescement de la personne représentée, ni du fait qu'il avait déjà purgé une peine pour un autre délit. La CEDH n'avait donc établi aucune violation de l'article 10 de la Convention par l'injonction d'interdiction prononcée par la juridiction nationale.

Dans les cas de crimes à sensation, les médias couvrent souvent l'affaire dès la phase de « recherche du coupable ». Le plus souvent, les contraintes à respecter dans les comptes rendus de la presse et de la radiodiffusion, ou, le cas échéant, dans d'autres médias audiovisuels, sont identiques. Nous présentons ci-après quelques jugements concernant les comptes rendus médiatiques :

Dans l'affaire *A. contre Norvège*, la CEDH considère que les reportages basés sur des présomptions de culpabilité constituent une violation de l'article 8 de la Convention. Dans le cadre de l'enquête de police visant à résoudre un crime commis contre deux enfants, la requérante avait été interrogée comme témoin. Par la suite, un journal avait publié un compte-rendu conçu de telle sorte qu'il laissait entendre que la requérante était suspectée. Bien que son nom ne fût pas mentionné, les personnes de sa connaissance auraient pu l'identifier au moyen des photos publiées et des détails concernant son domicile et son lieu de travail. La CEDH a établi que cette publication constituait une présomption de culpabilité particulièrement grave de la personne concernée et portait « préjudice à son intégrité morale et psychologique, ainsi qu'à sa vie privée. »

L'affaire mettant en cause le quotidien espagnol *El Mundo* concerne l'étendue du devoir de diligence des journalistes dans des comptes rendus faisant état de soupçons de transactions illégales à l'égard de la femme d'un président de tribunal⁴⁴. La CEDH n'a reconnu dans cette affaire aucune violation de l'article 8 de la CEDH. Elle estime que le journal a fait preuve de la diligence nécessaire dans ses recherches, puisqu'il a suffisamment vérifié ses sources : la véracité des données sur un disque anonyme avait été confirmée dans un entretien avec l'ancien comptable de l'entreprise. En outre, la version contraire des faits présentée par l'entreprise avait été intégrée dans le compte-rendu.

Dans ce contexte, il convient de noter que certaines données à caractère personnel sont couvertes par une protection spécifique garantie par le dispositif juridique : le devoir de confidentialité – en vue de protéger une relation de confiance particulière et /ou pour des raisons supérieures liées à l'intérêt public – découle, par exemple, de la relation entre un avocat et son client⁴⁵ (mais aussi entre médecin et patient, directeur de conscience et paroissien), relation qui est protégée par l'article 6 (droit à un procès équitable) et 8 de la Convention. Ainsi, on assiste régulièrement à des débats juridiques sur la question de savoir s'il est permis de rendre compte des affaires en cours en reproduisant littéralement (en partie) la lettre de l'avocat. La publication du seul fait qu'il existe une relation avocat-client affecte les intérêts de l'avocat et du client dont il a la charge. Néanmoins, la Cour suprême en Allemagne ne considère pas qu'il soit, d'une façon générale, illégal de publier de tels extraits⁴⁶. Il semble que les décisions correspondantes ont traité « uniquement » les droits de la personnalité et de l'exercice professionnel de l'avocat. Reste à savoir si le droit du client à la protection des données à caractère personnel prévaut sur le droit des médias à la liberté d'expression et sur la liberté des médias qui sont garantis par la loi.

Ces exemples illustrent les obligations de diligence qui incombent aux médias lors de leurs comptes rendus des procédures judiciaires ou administratives. Mais l'Etat lui-même est tenu, conformément à la jurisprudence établie de la CEDH, non seulement au respect du droit de la personnalité, mais à sa protection active. Par conséquent, il doit lutter de manière appropriée, dans sa sphère d'influence, contre les infractions éventuelles des médias. De ce point de vue, les formats d'émission de « télé-réalité », où les représentants des médias accompagnent le personnel des autorités publiques dans leurs interventions sur le terrain, posent certains problèmes. Cela concerne, par exemple, les

44) CEDH, arrêt du 21 septembre 2010, *Polanco Torres et Movilla Polanco contre Espagne*, n° 34147/06.

45) Voir en particulier Dean Spielmann, *Das anwaltliche Berufsgeheimnis in der Rechtsprechung des EGMR*, Österreichisches AnwBl. 2010, 34 et s., disponible sur : http://www.rechtsanwaelte.at/pdfsuche/10_anwbl0708.pdf ; de même que CJUE, arrêt du 14 septembre 2010, C-550/07, *Akzo*, par. 40 et s., 92 et s.

46) Voir BVerfG, arrêt du 18 février 2010, affaire 1 BvR 2477/08, http://www.bverfg.de/entscheidungen/rk20100218_1bvr247708.html

reportages vidéo sur les mesures de contrainte par voie de justice au domicile du débiteur, sur les contrôles de police au niveau de la circulation, les enquêtes criminelles et l'action des organismes sociaux ou des agences pour l'emploi⁴⁷. En matière de protection juridique des données, la mise à nu des individus qu'implique ce type de reportages fait apparaître un déséquilibre entre le droit du public à l'information et les droits de la personnalité de la personne concernée⁴⁸. Ce type de reportage est particulièrement problématique, car il semble que les autorités qui interviennent n'assurent pas suffisamment la protection des personnes concernées, qui sont déjà fragilisées par la situation imprévue ou par la brusque irruption des autorités. Sur ce point, l'Etat pourrait s'acquitter de son obligation positive de protection en veillant, au moins, à ce que ses agents informent la personne concernée sur ses droits et, en particulier, sur le caractère volontaire de sa participation à l'émission⁴⁹, avant que l'activité journalistique ne démarre.

Sur le Web 2.0, il est possible d'afficher ses opinions personnelles, dans le cadre des blogs ou des podcasts sans contraintes techniques, financières ou personnelles particulières. Selon les circonstances, les personnes privées qui exercent leur liberté d'expression doivent néanmoins respecter certaines obligations de vigilance. Ces obligations restent nettement en deçà du niveau d'exigences applicables aux médias, ainsi que l'a établi la *Bundesverfassungsgericht* (Cour fédérale constitutionnelle allemande - BVerfG) dans l'affaire suivante : un membre du conseil d'administration d'une association privée avait accusé dans un tract une multinationale chimique allemande de soutenir et de financer des responsables politiques « de droite et complaisants ». Ses propos s'appuyaient sur plusieurs reportages des médias concordants. La BVerfG a reconnu que la presse avait un « devoir particulier de diligence dans la diffusion de faits défavorables » ; cependant, pour un particulier, ce devoir ne s'applique qu'aux faits relevant « de son propre champ d'expérience et d'influence. » Lorsqu'il s'agit d'événements d'intérêt public intervenant dans « des domaines politiques et économiques dénués de transparence », l'individu est tributaire des comptes rendus des médias, puisque des recherches personnelles ne pourraient pas mettre à jour de preuve suffisante. Si on exigeait cela de lui, cela reviendrait à paralyser la liberté d'expression individuelle⁵⁰.

Dans les affaires *Thorgeirson*⁵¹ et *Marônek*⁵², la CEDH a statué sur une violation de la liberté d'expression par les auteurs de lettres ouvertes publiées dans les journaux. Les auteurs avaient tous été reconnus en dernière instance coupables de diffamation. Une éventuelle violation de la liberté de la presse n'a pas été soulevée et n'a donc pas fait l'objet d'un examen explicite. Mais la CEDH est manifestement partie du principe que la seule publication de lettres ouvertes par un organe de presse ne saurait en placer l'auteur sous la protection de la liberté de la presse. Inversement, l'obligation spécifique applicable aux médias professionnels de respecter les droits de la personnalité d'autrui ne devrait pas être étendue aux personnes qui n'exercent leur liberté d'expression que de façon occasionnelle – y compris et en particulier dans le cadre des nouveaux services du web participatif.

47) En ce qui concerne les délits (présumés ou réels) de célébrités, on a assisté ces derniers temps à une accumulation d'affaires dans lesquelles les services de poursuites judiciaires ont alimenté des reportages médiatiques épiquant clairement sur les droits de la personnalité des personnes concernées : cela englobe la présentation de l'ex-directeur du Fonds monétaire international, Dominique Strauss-Kahn, lors de son arrestation (sur la recevabilité de cette « perp walk » (exhibition publique d'un suspect) aux yeux de la loi américaine : <http://www.sueddeutsche.de/kultur/perp-walk-von-strauss-kahn-handschellen-zieren-jeden-verdacht-1.1098660>). On peut également citer les fuites de certains détails du dossier d'enquête contre le célèbre météorologue et présentateur de télévision Jörg Kachelmann (il a obtenu une injonction d'interdiction contre les médias, voir à ce sujet : <http://www.dr-bahr.com/news/presserecht/verbreitung-von-kachelmann-fotos-bei-hofgang-in-jva-rechtswidrig.html>) ainsi que l'arrestation et l'inculpation de la chanteuse d'un groupe allemand pour lésions corporelles graves au motif rendu public qu'elle avait eu des relations sexuelles non protégées alors qu'elle se savait atteinte du virus HIV. Voir à ce sujet Gernot Lehr, « Es darf nicht vorverurteilend berichtet werden » – Interview, *epd medien* 2011 (cahier 23), p. 3 et s.

48) Cf. Critique de la Conférence des responsables fédéraux et régionaux de la protection des données en soutien aux instances judiciaires pour les émissions de télé-réalité, Résolution du 24 juin 2010 et références citées : Die Landesbeauftragte für Datenschutz und Informationsfreiheit im Saarland, 23. Tätigkeitsbericht, Sarrebruck 2011, p. 123 f., disponible sur : http://www.landtag-saar.de/dms14/So14_0425.pdf

49) Voir sur ce point Robert Rittler, Autriche : « L'absence d'opposition à un reportage télévisé vaut consentement probant », IRIS 2010-1/8.

50) BVerfGE 85, 1, 22 ; par. 62 (réf. citées <http://www.servat.unibe.ch/dfr/bv085001.html#Rn062>).

51) CEDH, arrêt du 25 juin 1992, *Thorgeir Thorgeirson contre Islande*, n° 13778/88.

52) CEDH, arrêt du 19 juillet 2001, *Marônek contre Slovaquie*, n° 32686/96.

bb) L'accès aux comptes rendus par le biais des archives et moteurs de recherche

Même si le compte-rendu d'une procédure administrative ou judiciaire permettant l'identification de la personne concernée est autorisé, étant donné la jurisprudence existante, la question se pose de savoir pendant combien de temps ces comptes rendus peuvent être maintenus à disposition, par exemple, dans les vastes archives des actualités sur internet. Les affaires jugées précédemment portaient principalement sur les archives de presse en ligne. Le développement des bibliothèques multimédia, qui proposent sur internet pendant au moins un certain temps les contenus diffusés précédemment à la télévision linéaire, pose le même problème, mais à propos des contenus audiovisuels.

Récemment, le BGH allemand a eu plusieurs fois l'occasion⁵³ de trancher sur la question fondamentale de l'équilibre des intérêts en présence. Le meurtrier d'un acteur ayant bénéficié d'une libération conditionnelle en janvier 2008 avait porté plainte contre la publication d'un article paru le 12 avril 2005 sur un portail d'actualité en ligne qui déclarait, en mentionnant son nom complet, qu'un tribunal examinait la possibilité de révision du procès. Le BGH avait néanmoins conclu que le droit à l'information du public et le droit de la défenderesse à la liberté d'expression prévalaient sur le droit à la réintégration sociale du meurtrier. Le BGH estime qu'avec le recul croissant dû au temps écoulé depuis le crime, la réinsertion sociale du meurtrier prend de l'importance lors de la mise en balance des intérêts en jeu, mais que le préjudice lié à la mention nominative du meurtrier n'est toutefois pas significatif. L'article en cause constitue, selon le BGH, une présentation factuelle et objective de déclarations véridiques, il est classé comme « ancienne dépêche » dans la section des archives du portail et il faut lancer une recherche spécifique pour le consulter. La demande générale de suppression de tous les anciens articles traitant de ce crime et permettant l'identification de l'auteur constituerait une limitation abusive de la liberté d'expression et des médias.

Prochainement, la CJUE devra statuer sur la responsabilité des moteurs de recherche concernant les résultats affichés à l'écran suite à une recherche (en principe, il peut également s'agir de photos et de vidéos) : à la demande de plusieurs personnes, l'*Agencia Española de Protección de Datos* (Autorité espagnole de protection des données - AEPD) avait contraint l'exploitant du moteur de recherche Google à supprimer de ses résultats des liens vers des articles publiés en ligne longtemps auparavant, en vue d'assurer la protection des données à caractère personnel. Un cas particulièrement instructif mettait en cause un article datant de 1991 du quotidien espagnol *El País* au sujet d'une plainte contre un chirurgien esthétique suite à une erreur présumée de traitement. L'article paru ultérieurement qui rapporte de façon très succincte la mise hors de cause du chirurgien concernant toutes les charges qui pesaient contre lui figure dans les résultats du moteur de recherche à une place beaucoup moins visible que le premier article. Dans une décision du 4 février 2009⁵⁴, l'AEPD avait établi que l'article lui-même ne devait pas être supprimé. La Cour constitutionnelle espagnole a établi que la liberté d'information normalisée dans la Constitution espagnole prend le pas sur le droit à la vie privée, dès lors que les faits rapportés sont véridiques et qu'ils présentent un intérêt public. Contrairement à un article individuel, la composition de l'index de recherche de Google et la mise à disposition des résultats des recherches ne relèvent pas de la liberté d'information. Google avait attaqué cette décision devant l'*Audiencia Nacional*, qui avait saisi la CJUE de cette affaire⁵⁵. Google craint que le « droit à l'oubli », qui est actuellement en discussion, ne se révèle être un moyen de censure pour les documents gênants et que le juste équilibre entre la protection des droits de la personnalité et la liberté d'expression, de la presse et de l'information ne soit modifié au détriment de ces dernières.

53) *Op. cit.* (note 22). Voir également CEDH, arrêt du 10 mars 2009, *Times Newspapers contre Royaume-Uni* 3002/03 et 23676/03, dans lequel la Cour réfute une violation de l'article 10, paragraphe 1 de la Convention, au motif que la demande d'intégrer aux articles incriminés pour diffamation, contenus dans les archives en ligne du journal, une référence à la procédure judiciaire y afférente ne limite pas la liberté d'expression de façon disproportionnée - la requête ne porte pas, d'ailleurs, sur le retrait intégral des articles de ces archives en ligne.

54) AEPD, Résolution du 4 février 2009, n° R/00155/2009, disponible sur : http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2009/common/pdfs/TD-01335-2008_Resolucion-de-fecha-04-02-2009_Art-ii-culo-17-LOPD_Recurrida.pdf

55) Voir Josh Halliday, « Europe's highest court to rule on Google privacy battle in Spain », 1^{er} mars 2011, <http://www.guardian.co.uk/technology/2011/mar/01/google-spain-privacy-court-case>

cc) Comptes rendus sur diverses célébrités

Dans l'affaire *Caroline de Hanovre*, la CEDH a condamné la publication de photographies issues de la vie privée de la princesse sur la base de l'article 8 de la Convention. La Cour a confirmé que la publication de photographies montrant la requérante dans sa vie quotidienne était protégée par le droit à la liberté d'expression, tout en soulignant cependant que cette publication portait également atteinte à sa vie privée. L'élément déterminant pour trouver le juste équilibre entre ces droits fondamentaux concurrents consiste à savoir si la photo contribue à un débat public d'intérêt général⁵⁶. Or, la CEDH considère que les photos privées d'une « personne célèbre » qui ne joue aucun rôle politique officiel ne remplissent pas ce critère (« ne saurait [...] contribuer à un quelconque débat d'intérêt général pour la société »). Le public n'a aucun intérêt légitime à savoir où se trouve la requérante et comment elle se comporte dans sa vie privée. L'intérêt public, pour autant qu'il existe, ne saurait, en l'espèce, entrer en concurrence avec le droit de la requérante à une protection effective de sa vie privée.

En revanche, dans l'affaire *Max Mosley*, la CEDH établit que l'article 8 de la Convention n'impose pas d'informer au préalable les personnes concernées de la publication prévue d'un article à leur sujet. Dans ce cas précis, l'hebdomadaire britannique *News of the World* avait fait enregistrer secrètement des photos et des séquences vidéo relevant de la vie privée de Max Mosley, l'ancien président de la Fédération Internationale de l'Automobile, où il apparaissait en compagnie de prostituées. Les photos ont été publiées par le journal sur internet, accompagnées d'un article sur les activités sexuelles du requérant. Mosley a porté plainte devant la CEDH pour violation de la vie privée, qui, conformément à la législation britannique, n'aurait pu être préservée que par une injonction d'interdiction (*injunction*) ordonnée par un tribunal. Etant donné qu'aucune disposition dans la loi britannique ne prévoit une notification préalable de la personne concernée, il n'a pas pu en avoir connaissance et, partant, aucune *injunction* n'a pu être requise. Or, ceci est contraire à l'article 8 de la Convention. La CEDH a reconnu que la protection des droits d'autrui revêt une importance particulière, notamment dans les médias audiovisuels, car ils ont souvent un impact beaucoup plus direct et plus profond que la presse. La CEDH ne reconnaît dans la publication des photos en cause « aucune contribution supplémentaire possible » à un débat d'intérêt général. Il semble que ces documents aient été intégrés à l'article dans le seul but de satisfaire la curiosité du public et d'humilier la partie requérante. Néanmoins, la CEDH considère que l'article 8 de la Convention n'impose pas d'obligation légale d'informer préalablement la partie concernée. La mise en balance doit tenir compte de la portée limitée des restrictions à la liberté de presse en vertu de l'article 10 de la Convention. La CEDH voit un risque général lié aux effets dissuasifs, risquant d'entraîner une censure préalable dans le domaine des comptes rendus politiques et du journalisme d'investigation, spécifiquement protégé par la Convention. Par conséquent, la Cour n'a pas retenu de violation de l'article 8 de la Convention⁵⁷.

En droit polonais, il existe pour les enregistrements audio et vidéo une obligation de consentement préalable qui s'est avérée problématique dans l'affaire suivante : le rédacteur en chef d'un journal avait été condamné pour la publication d'extraits d'une interview d'un responsable politique. Ce dernier avait accepté l'interview, mais refusé d'accorder son consentement préalable, prévu par la loi, à la publication d'une version remaniée et très condensée. Par la suite, le journal a publié des extraits tirés des séquences originales de l'interview. La CEDH a considéré que la condamnation du rédacteur en chef pour avoir manqué à l'obligation d'obtenir le consentement préalable constituait une violation de l'article 10 de la Convention, car cette condamnation peut avoir un effet dissuasif et disproportionné sur la presse. La CEDH a pris en compte, dans son examen, le caractère volontaire de l'interview et le fait que la loi sur la presse polonaise prévoit une sanction sans prendre en compte le contenu des déclarations. Ceci n'est pas conforme aux principes de la jurisprudence relative à l'article 10 de la Convention, en vertu de laquelle les limites de la critique acceptable sont plus larges à l'égard des personnalités politiques que des particuliers. L'obligation de consentement constituerait une « carte blanche » permettant aux responsables politiques de dissimuler leurs propos inopportuns. En outre, le droit polonais prévoit d'autres moyens pour assurer une protection *a posteriori* contre les atteintes à la vie privée. La CEDH a jugé paradoxal que la loi sur la presse autorise la publication sans

56) CEDH, arrêt du 24 juin 2004, *von Hannover contre Allemagne*, n° 59320/00, par. 52, 59 et s., 76.

57) CEDH, arrêt du 10 mai 2011, *Mosley contre Royaume-Uni*, n° 48009/08.

autorisation préalable d'interviews remaniées ou simplement co-rédigées, tandis que les déclarations effectives et concrètes sont soumises à l'approbation de la personne concernée⁵⁸.

Au Royaume-Uni, la pratique des « *super-injunctions* » s'est retrouvée récemment au cœur du débat sur l'intérêt public⁵⁹. Ce type d'ordonnance judiciaire interdit non seulement de faire un compte rendu sur une affaire particulière sous une forme permettant l'identification de la personne concernée (voir à cet égard le rôle de la simple *injunction* dans l'affaire Mosley), mais aussi de mentionner le fait même qu'une ordonnance a été prononcée. Par conséquent, une injonction d'interdiction ne devient généralement publique que si elle est levée ou – ce qui est légalement possible en raison du privilège parlementaire – débattue à la Chambre des communes. La violation d'une telle ordonnance peut être punie par une peine maximum de deux ans d'emprisonnement. En 2011, les déboires extra-conjugaux d'un joueur de football britannique ont suscité une attention particulière. Cet homme aurait eu une liaison avec un célèbre mannequin gallois. Craignant que sa maîtresse ne porte cette affaire devant les médias, il a rencontré celle-ci à deux reprises dans des hôtels différents, mais a refusé de lui verser une somme d'argent qu'elle lui aurait demandée. Apparemment informés de ces rencontres, des journalistes de presse ont photographié le footballeur alors qu'il se rendait à ces rendez-vous. Ce dernier a obtenu que soit rendue une *super-injunction* pour que son identité ne soit pas mentionnée dans cette affaire. Mais un journaliste opérant de façon anonyme a enfreint cette ordonnance et publié sur le service de messagerie Twitter un communiqué faisant état de la liaison présumée du joueur de football en le citant par son nom.

Par ailleurs, en mars 2011, une forme encore plus restrictive « d'ordonnance-bâillon » a été rendue publique⁶⁰ : l'*hyper-injunction* interdit même la personne concernée de divulguer l'objet du litige de l'*injunction* à un député parlementaire.

c) Publication d'informations obtenues illégalement

Les sujets autorisés ou non à faire l'objet d'un compte-rendu dans les médias dépendent également, selon les circonstances, de la façon dont les informations ont été obtenues. Dans l'affaire *Fressoz et Roire*, la CEDH s'est penchée sur la question de savoir si la divulgation de documents confidentiels du fisc sur les revenus de l'ancien PDG de Peugeot SA était justifiée en vertu de l'article 10 de la Convention⁶¹. La partie requérante avait publié une copie des documents qui lui avaient été remis de façon anonyme, ce qui lui avait valu une condamnation. La CEDH a estimé que l'information du public sur le niveau de revenu constituait, à l'époque, une contribution au débat public sur les salaires de l'entreprise dans le cadre d'une négociation collective. Mais l'élément déterminant, pour la décision de la CEDH, porte sur le fait qu'en vertu du droit français, les informations contenues dans les dossiers fiscaux sont accessibles aux contribuables de la même circonscription. En outre, les salaires des directeurs de grandes entreprises telles que Peugeot sont régulièrement publiés dans les magazines financiers, et le caractère fondamentalement légal de cette publication est incontesté. La CEDH a estimé qu'une condamnation due au simple fait de publier ces documents porte préjudice à la liberté de la presse⁶².

58) CEDH, arrêt du 5 juillet 2011, *Wizerkaniuk contre Pologne*, n° 18990/05.

59) Master of the Rolls, Report of the Committee on Super-Injunctions v. 20. Mai 2011, disponible sur : <http://www.judiciary.gov.uk/Resources/JCO/Documents/Reports/super-injunction-report-20052011.pdf>

60) Voir Steven Swinford, « 'Hyper-injunction' stops you talking to MP », 21 mars 2011, <http://www.telegraph.co.uk/news/uknews/law-and-order/8394566/Hyper-injunction-stops-you-talking-to-MP.html>

61) CEDH, arrêt 21 janvier 1999, *Fressoz et Roire contre France*, n° 29183/95.

62) Contrairement à la Chambre des députés italienne l'an dernier : après la publication de rapports de police sur les écoutes téléphoniques du premier ministre, le parlement a adopté un projet de loi qui limitait nettement les mesures de surveillance des télécommunications et sanctionnait la publication de comptes rendus d'écoutes téléphoniques de même que la divulgation d'extraits de dossiers d'enquête ; pour plus de détails sur l'origine de ce débat, voir Michael Brown, « Abhörprotokolle belegen Manipulation », disponible sur : <http://www.taz.de/!7966/>, et le rapport APA, « Rechtsanwälte bestreiten Berlusconi-Verwicklung in Fernsehaffäre », <http://derstandard.at/1310511702569/Italien-Rechtsanwaelte-bestreiten-Berlusconi-Verwicklung-in-Fernsehaffaere> . Ce projet de loi permettrait de restreindre sensiblement la possibilité de faire des comptes rendus sur les procédures pénales. Après avoir été amendé par le sénat, le projet de loi est revenu au parlement ; voir le rapport de la séance n° 529 de la chambre des députés du 5 octobre 2011, p. 1 et s., <http://www.camera.it/412?idSeduta=529&resoconto=steno-grafico&indice=alfabetico&tit=00040&fase=#sed0529.stenografico.tit00040>.

Quinze ans auparavant, la Cour fédérale constitutionnelle allemande avait déjà statué sur une plainte constitutionnelle du groupe Axel Springer AG contre le journaliste d'investigation *Günter Wallraff* en déclarant que la publication d'informations obtenues ou acquises de façon illégale est également couverte par la protection de la liberté d'expression. Il convient néanmoins d'éviter, en principe, de publier un article dont l'auteur a obtenu les informations « illégalement par tromperie » et entend les utiliser « au détriment de la victime de la tromperie ». La seule exception applicable concerne les cas où « l'importance de l'information au regard de la nécessité d'éclairer le public et de contribuer à la formation de l'opinion publique l'emportent clairement sur les inconvénients qu'impliquent la violation du droit pour la personne concernée et l'application (réelle) de la législation. » Ce qui n'est « généralement pas le cas » lorsque les informations font référence à des situations ou des comportements qui, pour leur part, ne sont pas illégaux⁶³.

Les affaires mentionnées ci-dessus concernent le traitement de données obtenues illégalement par leur publication dans les médias.

Il est intéressant de noter que la Directive 95/46/CE ne distingue pas, d'une façon générale, si les données sont, ou étaient, à caractère public ou privé. Dans l'affaire *Satakunnan et autres*, l'avocat général fait valoir que dans le cas de données déjà publiées, le droit à la vie privée cède le pas, en règle générale, à la liberté d'expression. Néanmoins, la personne concernée peut être protégée contre la poursuite du traitement et de la diffusion, notamment dans le cas d'informations mensongères, outrageantes, ou d'informations relevant de la vie privée. Le pouvoir discrétionnaire des Etats membres « ne doit pas conduire à ce que les dérogations à la protection des données légitiment une restriction manifestement disproportionnée du droit à la vie privée ⁶⁴. »

La publication d'une vidéo dans un environnement Web 2.0 a été jugée par un tribunal de Milan en 2010⁶⁵ : il s'agissait de déterminer si quatre responsables de Google avait commis une infraction en s'abstenant d'effacer pendant plusieurs semaines une vidéo montrant une personne souffrant du syndrome de Down victime de maltraitance. La partie défenderesse alléguait que leur plateforme *Google Video* a le statut de simple hébergeur et n'est pas responsable des contenus téléchargés⁶⁶. Toute personne qui télécharge des vidéos est liée par les conditions générales d'utilisation et, notamment, par les dispositions concernant la protection de la vie privée. Le tribunal a suivi le raisonnement selon lequel un fournisseur qui se contente de délivrer un simple « service de connexion » n'est pas tenu de vérifier les contenus téléchargés. Toutefois, il doit informer les utilisateurs sur leurs obligations en matière de respect des droits de la personnalité. En particulier, le tribunal a dénoncé le fait que la personne photographiée n'avait pas consenti à la publication des données à caractère personnel la concernant. Le tribunal reconnaît certes que Google ne peut pas vérifier l'existence d'un consentement dans tous les cas, néanmoins, l'entreprise doit au moins s'assurer que tout utilisateur téléchargeant du contenu et intervenant simultanément comme un fournisseur de contenu (cette double fonction étant également appelée « *prosommateur* ») confirme l'existence d'un tel consentement. Cela pourrait, par exemple, se faire au moyen d'un avis d'information approprié sur la protection des données s'affichant avant tout téléchargement d'une vidéo et devant être confirmé par l'utilisateur⁶⁷.

63) BVerfGE 66, 116 (et références citées <http://www.servat.unibe.ch/dfr/bv066116.html>).

64) Conclusions de l'avocat général, *Satamedia*, *op. cit.*, par. 124.

65) Valentina Moscon, « Le tribunal de Milan rend son verdict dans l'affaire Google Video », IRIS 2010-6/35.

66) Voir l'art. 14 de la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») JOUE du 17 juillet 2000, L 178, p. 1.

67) L'exploitant d'un forum d'accès public au registre du commerce irlandais, sur lequel un utilisateur avait publié les données à caractère personnel d'un tiers a néanmoins été considéré responsable, par un tribunal allemand, du traitement des données, car la mise à disposition des contributions sur le forum contribuait également pour le moins « à ses intérêts commerciaux propres » (voir OLG Hambourg, arrêt du 2 août 2011, 7 U 134/10, et références citées : <http://www.aufrecht.de/index.php?id=6988>). Toutefois, dans ce cas concret, l'exploitant a été autorisé à permettre la consultation de cette contribution, car il a été établi qu'il y avait un intérêt public justifiant la divulgation publique des données conformément à l'article 28, paragraphe 2 de la BDSG (loi allemande sur la protection des données) à titre d'information aux fins d'éclairer les consommateurs. L'OLG estime que la même conclusion découle de la mise en balance de la liberté d'expression et du droit général de la personnalité.

III. Les médias et la protection des données des utilisateurs

Les données à caractère personnel jouent également un rôle dans les relations entre les médias et leurs utilisateurs. Contrairement au cas du traitement des données à des fins journalistiques, les médias utilisent les données des utilisateurs aux fins de commercialisation des contenus. Dans ce cadre (comme dans toutes les autres relations non journalistiques), ils doivent se conformer à la réglementation en matière de protection des données⁶⁸. Outre la Directive 95/46/CE relative à la protection générale des données, la directive 2002/58/CE⁶⁹ comporte des règles spécifiques sur la protection des données dans les communications électroniques. Dans le cadre de la révision du « Paquet Télécom⁷⁰ », cette directive a été modifiée par de nouvelles dispositions qui sont inscrites dans la directive 2009/136/CE⁷¹. Ces modifications englobent notamment l'article 5, paragraphe 3 de la directive 2002/58/CE, en vertu duquel les informations telles que les cookies peuvent uniquement être stockées ou consultées sur le terminal de l'utilisateur avec son consentement. Nous abordons dans ce qui suit les effets spécifiques de ces dispositions sur les activités des médias dans la fourniture et la commercialisation de contenus.

1. Les médias traditionnels

Les consommateurs de médias font l'objet de divers traitements de données. L'utilisation totalement anonyme des médias est techniquement possible, par exemple lors de l'achat d'un quotidien dans un kiosque ou de la réception gratuite par voie terrestre ou par satellite de programmes de radiodiffusion. Mais pour des raisons pratiques ou juridiques, les médias ont souvent recours à certains modèles commerciaux faisant intervenir un traitement des données à caractère personnel des usagers. Quiconque souhaite avoir son quotidien livré à domicile doit communiquer au moins son nom et son adresse. Le choix de certains canaux de distribution, tels que la télévision par câble, implique une relation contractuelle avec le fournisseur de services de transmission (c'est-à-dire le câblo-opérateur ou l'opérateur de plateforme) qui nécessite la communication des coordonnées⁷² des clients pour assurer la prestation et la facturation des services.

Les fournisseurs de contenus sont, eux aussi, souvent tributaires de ces données : si le modèle économique prévoit le financement d'une offre de médias par l'utilisateur, ce dernier doit pouvoir être identifié. Lorsque le montant des services facturés est basé sur l'usage effectif desdits services (comme pour la télévision à péage), il faut également procéder au traitement des données portant sur la consommation (données relatives au trafic⁷³). Il en va de même pour les services audiovisuels proposant des services interactifs supplémentaires : ils doivent pour cela disposer d'un canal de

68) Pour une présentation détaillée de la situation au regard du droit britannique, voir Ian Walden/Lorna Woods, « Broadcasting Privacy », *Journal of Media Law* 2011 (cahier 1), p. 117 et s.

69) 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 (directive « vie privée et communications électroniques ») JOUE du 31 juillet 2002, L 201, p. 37.

70) Voir à ce sujet Sebastian Schweda, « Révision du "Paquet Télécom" : un nouvel élan pour les médias audiovisuels ? » dans : Observatoire européen de l'audiovisuel (Ed.), *Régulation des communications : entre infrastructure et contenu*, IRIS plus 2009-10.

71) Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n°2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, JOUE du 18 décembre 2009, L 337, p. 11.

72) On entend par coordonnées les données à caractère personnel (au sens visé à l'art. 2, par. a de la Directive 95/46/CE, cf. ZOOM, section II 2.a) de l'utilisateur ou de l'abonné, dont le traitement par le prestataire de service est nécessaire pour mettre en œuvre le lien contractuel, comme, par ex., le nom, l'adresse, et éventuellement les coordonnées bancaires.

73) Voir la définition de l'art. 2, par. b de la Directive 2002/58/CE : les « données relatives au trafic » sont « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ».

retour qui transfère les informations de l'utilisateur vers le fournisseur. C'est le cas, par exemple, de la télévision connectée⁷⁴.

Dans certains Etats, le consommateur (potentiel) des offres publiques est associé à leur financement. Lorsque l'assujettissement au paiement dépend de certaines conditions, il faut également traiter des données à caractère personnel pour identifier les contribuables et vérifier qu'ils s'acquittent convenablement de cette redevance. Ce principe s'applique aussi bien à une redevance obligatoire découlant de la capacité à recevoir les services qu'à une taxe établie en fonction des foyers⁷⁵.

2. Les « nouveaux » médias

a) Principes techniques du traitement des données et classification juridique

Pour la mise à disposition des contenus multimédia, le traitement des données peut, dans la plupart des cas, se limiter aux simples coordonnées. L'analyse du comportement de l'utilisateur n'est nécessaire que si les frais d'accès sont calculés en fonction du type ou du volume d'utilisation. Ce principe s'applique également aux « nouveaux » médias proposés sur les réseaux de communications numériques. L'utilisation de la transmission des données par paquets, comme sur internet ou les autres réseaux basés sur IP, requiert et autorise l'identification de chaque terminal connecté par une adresse unique. Cela permet à l'information de trouver son chemin entre l'expéditeur et le destinataire. Pour éviter autant que possible les erreurs de transmission, chaque paquet de données reçu sans erreur doit être confirmé par le destinataire. Cela signifie que, dès la transmission, il est possible de savoir sur quel terminal et sur quelle période les contenus sont réceptionnés⁷⁶.

Dans ce contexte, les entreprises intégrées verticalement qui opèrent à la fois comme fournisseurs de contenus et comme fournisseurs d'accès internet ou opérateurs de plateforme (à l'instar des fournisseurs de télévision par internet qui commercialisent leurs services via leur propre liaison ADSL) ont la possibilité de mettre en relation les coordonnées des utilisateurs, les données relatives au trafic et les données de consommation⁷⁷. Les profils d'utilisateurs ainsi créés permettent à ces entreprises de connaître quels contenus de leurs propres offres ont été consommés par quelle connexion et à quel moment.

Contrairement aux canaux de transmission traditionnels, les canaux de communication bidirectionnelle fournissent également un canal de retour de façon simultanée : la télévision interactive, ou la consommation de médias à la demande (par exemple la vidéo à la demande) sont considérablement facilitées par les technologies de communication par paquets. L'utilisateur individuel n'a accès aux contenus que s'il s'identifie au moins auprès de son opérateur de réseau – cela s'applique même lorsque les services sont proposés selon le procédé de la multidiffusion⁷⁸.

74) Voir à ce sujet Sebastian Artymiak, « Introduction à différents types de services audiovisuels à la demande », dans : IRIS Spécial, *La réglementation des services audiovisuels à la demande : chaos ou cohérence ?*, Observatoire européen de l'audiovisuel (Ed.), Strasbourg 2011 (à paraître).

75) Voir Christian M. Bron, « Le financement et le contrôle des offres des radiodiffuseurs de service public », dans : Observatoire européen de l'audiovisuel (Ed.), *Médias de service public : pas de contenu sans financement*, IRIS plus 2010-4.

76) Dans l'affaire *Promusicae*, l'avocat général classe les adresses IP dynamiques attribuées comme des données relatives au trafic et (à tout le moins) les informations découlant de l'attribution d'adresses IP aux abonnés comme des données à caractère personnel (Voir Conclusions de l'avocat général du 18 juillet 2007, C-275/06, *Productores de Música de España (Promusicae) contre Telefónica de España SAU*, par. 61 et 63).

77) Sur la base de l'article 15 de la loi allemande sur les télémédias, les informations à caractère personnel d'un utilisateur recouvrent les informations qui sont nécessaires pour permettre l'utilisation et la facturation d'un service de médias, comme, par exemple, les informations permettant d'identifier l'utilisateur, les horaires d'utilisation et les informations concernant les contenus consultés.

78) Dans le cadre de la multidiffusion, les contenus sont transmis depuis un diffuseur vers plusieurs destinataires. A la différence d'une liaison point à point entre deux terminaux, le signal doit être envoyé en une seule fois, mais il peut être reçu par plusieurs récepteurs. Mais à la différence de la radiodiffusion, il ne suffit pas, pour activer la réception, de sélectionner le canal de transmission correspondant sur un récepteur prêt à cet effet, il faut procéder préalablement à une connexion auprès du service de transmission.

Pour l'utilisation en mode nomade, les services de télévision linéaires sont souvent transmis par les technologies numériques de transmission de type DVB (transmission numérique terrestre). Ces normes de transmission ne s'appliquent généralement pas aux communications bidirectionnelles, mais à la radiodiffusion classique, au sens où un signal radio est émis « à destination de tous ». Des services interactifs sont disponibles, sous réserve de l'utilisation d'un terminal adapté permettant également l'accès aux réseaux mobiles (GSM/UMTS). Ces réseaux offrent à l'utilisateur un canal de retour disponible sur le même terminal. En revanche, lorsque des contenus audiovisuels sont visionnés via le réseau UMTS ou d'autres accès à internet sans fil (GPRS, WLAN, WiMAX), la transmission des signaux de télévision a lieu d'emblée sur la base d'une connexion bidirectionnelle.

Sur les couches inférieures et supérieures du protocole (selon le modèle OSI), l'utilisation d'un service de médias génère souvent d'autres données permettant l'identification, par exemple lors d'un changement de l'adresse IP ; sur les couches des applications, en particulier, il est possible d'affecter une classification à un terminal via des cookies (HTTP ou navigateur), utilisés de longue date : un site consulté par un utilisateur stocke un fichier sur l'ordinateur de ce dernier, et peut y accéder lors d'une prochaine visite sur ce même site ou sur un autre site de l'opérateur. Les *flash cookies*, utilisés dans le cadre de l'utilisation très répandue de la technologie *Flash* pour afficher des contenus audiovisuels, permettent également un suivi de l'utilisation d'un ordinateur particulier. Enfin, une étude a montré⁷⁹ que les opérateurs de sites internet – y compris, jusqu'à récemment, le portail vidéo américain *Hulu.com* et le site de musique *spotify.com* – utilisent des technologies, encore méconnues pour la plupart, qui permettent de restaurer les cookies ayant été supprimés (*Cookie-Respawning*) et d'identifier de façon permanente le navigateur (« cookies permanents »).

Des informations complémentaires sont disponibles par le biais de la « lecture » de la configuration en place du navigateur et du système, que le navigateur communique à chaque ouverture de page et qui, dans de nombreux cas, permet une localisation très précise du terminal. Grâce à une procédure d'alignement qui existe sur certains navigateurs et qui permet de comparer les sites visités précédemment avec ce navigateur et une liste de sites connus, l'exploitant d'un site pour également savoir si un utilisateur a déjà consulté l'offre de la concurrence⁸⁰. Des outils de suivi tels que *Google Analytics* offrent aux fournisseurs la possibilité d'analyser les connexions d'un utilisateur spécifique sur son site internet. Le caractère légal de ces outils est diversement apprécié⁸¹.

Au-dessous de la « couche réseau », sur laquelle le protocole internet assure le routage des paquets de données, se trouve la couche de sécurité basée sur le modèle OSI. C'est à ce niveau que se déroule le contrôle de l'accès aux adaptateurs réseau par le biais des adresses MAC⁸² internationales, uniques et spécifiques à l'appareil. Depuis quelques temps, Google collecte les adresses MAC des bornes de réseaux locaux sans fil (*Wireless Local Area Networks* – WLAN) du monde entier dans le cadre de ses déplacements pour le service photo *Street View* et avec l'aide de smartphones sous Android. Les utilisateurs de portables sont ainsi en mesure de déterminer leur propre position sans GPS. En juin 2011, il a été rapporté que Google avait également inclus en partie des adresses MAC d'ordinateurs et de smartphones privés dans sa base de données⁸³.

En raison du lien étroit entre les utilisateurs et leur appareils (en particulier les terminaux mobiles), le CEPD et le groupe de travail Article 29 réunissant les représentants des autorités

79) Voir le compte-rendu sur : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 . Les techniques utilisées sont basées principalement sur le stockage (intermédiaire) des informations du cookie dans d'autres zones de stockage accessibles au navigateur sur l'ordinateur local. Si un cookie HTTP d'une page utilisant ces techniques est supprimé, ses informations peuvent être lues à partir des autres zones de stockage, par exemple avec JavaScript et le cookie HTTP sera rétabli, sans que l'utilisateur ne s'en rende compte ou n'y consente.

80) Voir à ce sujet: Dongseok Jang et al., « An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Application », disponible sur : <http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf>

81) Voir *Thomas Hoeren*, « Google Analytics – datenschutzrechtlich unbedenklich? », ZD 2011, 3 et s., ainsi que récemment <http://www.sueddeutsche.de/digital/umstrittener-web-statistikdienst-datenschuetzer-erlaubt-einsatz-von-google-analytics-1.1144297>

82) MAC est l'acronyme de *Media Access Control*.

83) Voir : « WLAN-MAC-Adressen: Googles langes Gedächtnis », 16 juin 2011, <http://www.heise.de/netze/meldung/WLAN-MAC-Adressen-Googles-langes-Gedaechtnis-1261893.html>

nationales chargées de la protection des données considèrent que la géolocalisation d'adresses MAC constitue des données à caractère personnel. En vue d'instaurer un juste équilibre entre les droits concurrents, le groupe de travail Article 29 se déclare favorable à la mise en place de garanties suffisantes pour les personnes concernées par le traitement des données, comme, par exemple, la possibilité d'exercer un droit d'opposition (*opt-out*) simple et permanent sans fournir de données supplémentaires. De même, le CEPD estime que l'identification d'une borne de réseau (*Single Station Identifier* - SSID) sans fil ne devrait pas être traitée à des fins de géolocalisation⁸⁴.

b) *Les intérêts du secteur privé dans l'utilisation des données et le cadre juridique applicable*

Les données traitées en lien avec la fourniture de contenus peuvent être utilisées à des fins diverses qui dépassent la simple garantie d'une connexion conforme pour assurer une prestation de services. L'utilisation des données présente surtout un intérêt crucial pour les fournisseurs de contenus, car elles leur servent souvent à facturer des services payants.

Mais il existe également des intérêts commerciaux liés à l'utilisation des données avec les services gratuits : les services de médias sur internet sont souvent financés exclusivement par la publicité. En contrepartie de leur contribution financière, les annonceurs attendent un ciblage ajusté au plus près de leur clientèle. L'identification des utilisateurs sur les réseaux où transitent les paquets de données et le suivi de leurs activités sur une période prolongée permettent la création de profils d'utilisateurs et peuvent servir à la publicité comportementale. Etant donné que les opérations de publicité comportementale sont considérées comme plus prometteuses que la publicité ciblée en fonction des groupes cibles, les supports publicitaires peuvent généralement obtenir des revenus plus élevés⁸⁵.

Du point de vue de la protection des données, cette forme de publicité, appelée « publicité comportementale en ligne », suscite certaines réserves. Le CEPD considère que l'application systématique de telles techniques constitue une « pratique hautement intrusive »⁸⁶. Il dénonce, dans ce contexte, « l'érosion des droits fondamentaux et une défaillance du marché. » Selon lui, certains intérêts publics n'ont pas été suffisamment préservés, jusqu'à présent, lors du développement d'internet. Pour remédier à cette situation, le CEPD préconise des mesures correctives juridiques, techniques et d'autorégulation⁸⁷.

84) Groupe de travail Article 29 sur la protection des données, Opinion 13/2011 on Geolocation services on smart mobile devices du 16 mai 2011, WP 185, disponible sur : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf , p.17.

85) Concernant les conditions techniques et économiques, voir l'Avis 2/2010 du 22 juin 2010 sur la publicité comportementale en ligne, WP 171 du groupe de travail Article 29 sur la protection des données: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_fr.pdf, p. 4 et s.

86) CEPD, Conférence du 7 juillet 2011 à l'université d'Édimbourg, faculté de droit, « Refuser le suivi des consommateurs ou suivre la voie actuelle? – Les implications de la publicité comportementale en ligne sur la vie privée », disponible sur : http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2011/11-07-07_Speech_Edinburgh_FR.pdf, p. 8.

87) Citons à cet égard les initiatives de l'*European Advertising Standards Alliance* (voir « EASA Best Practice Recommendation on Online Behavioural Advertising », 13 avril 2011, http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download) et de l'*Interactive Advertising Board Europe* (« IAB Europe EU Framework for Online Behavioural Advertising », http://www.iabeurope.eu/media/51925/iab%20europe%20oba%20framework_merged%20ii.pdf). Néanmoins, le CEPD considère que c'est insuffisant, du moins en ce qui concerne l'utilisation de cookies, car ces initiatives ont tendance à appliquer davantage le modèle actuel de « droit d'opposition » (*opt-out*) que l'approche privilégiant « l'adhésion » (*opt-in*) qui est préconisée par la directive 2009/136/CE ; voir *ibid*, p. 6. Le Groupe de travail Article 29 sur la protection des données a également critiqué l'initiative comme insuffisante (voir la lettre du Groupe de travail Article 29 sur la protection des données du 3 août 2011, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf). En ce qui concerne la protection des mineurs, certains fournisseurs de réseaux sociaux, notamment Facebook, MySpace et YouTube, se sont engagés à proposer des réglages facilement détectables et accessibles pour protéger la vie privée, et à classer les profils des mineurs par défaut comme « privés » ; voir « Socialisation sur internet : accord entre les grands sites par l'entremise de la Commission », Communiqué de presse du 10 février 2009, IP/09/232, <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232&format=HTML&aged=1&language=FR&guiLanguage=fr>

Les annonceurs peuvent cibler leur public non seulement avec la publicité diffusée sur les offres de tiers, mais aussi au moyen de leurs propres services. La campagne de la brasserie américaine *Budweiser* a focalisé récemment l'attention du public : en août 2011, le Groupe affichait sur sa page Facebook britannique une rencontre du club de football *Ascot United*, encore peu connu jusque-là. Ceux qui voulaient regarder le match devaient cliquer sur le bouton « J'aime » de la page⁸⁸.

Cette interface permet aux utilisateurs enregistrés sur les sites *Facebook* d'annoncer publiquement sur un éventail de plus en plus large de sites Internet leur soutien au contenu d'une page ou à son auteur. Or, du point de vue de la protection des données, cela pose un problème, puisque même les données des utilisateurs non-inscrits sur Facebook mais qui visitent un site doté de ce type de bouton intégré peuvent faire l'objet d'un traitement.

On peut déjà contester le simple fait que la législation européenne en matière de protection des données soit applicable au traitement des données opéré par des groupes américains tels que *Facebook*. Si tel est le cas, on peut ensuite s'interroger sur le droit qu'il convient d'appliquer : le droit de l'Irlande, où *Facebook* a établi son siège européen, ou du pays dans lequel réside l'utilisateur⁸⁹? Indépendamment de ces considérations, l'*Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein* (Centre régional indépendant de protection des données du Schleswig-Holstein – ULD) a désormais les fournisseurs de contenus qui équipent leur page du bouton « J'aime » dans le collimateur : selon son analyse, l'intégration de cette interface sur un site internet hébergé en Allemagne est contraire au droit allemand et au droit européen en matière de protection des données⁹⁰. L'ULD dénonce également une violation de l'article 5, paragraphe 3 de la directive 2002/58/CE. La simple vue du bouton en question entraîne le stockage de cookies et de l'adresse IP, ainsi que le traitement des informations spécifiques au navigateur et autres données sans le consentement effectif de l'utilisateur. L'autorité a demandé aux opérateurs de sites concernés de supprimer le bouton d'ici fin septembre 2011 sous peine de se voir infliger jusqu'à 50 000 EUR d'amende.

En ce qui concerne, en particulier, l'utilisation de cookies et d'autres mesures de stockage ou de récupération d'informations sur le terminal de l'utilisateur, l'article 5, paragraphe 3 de la directive 2002/58/CE dispose :

« Les Etats membres garantissent que l'utilisation de réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur ne soit permise qu'à condition que l'abonné ou l'utilisateur ... ait donné son consentement »

Le consentement ne peut faire défaut qu'en cas de stockage ou d'accès techniques visant exclusivement à effectuer la transmission d'une communication ou s'avérant strictement nécessaires à la fourniture d'un service. En outre, l'article 5, paragraphe 3, phrase 1 de la directive 2002/58/CE prévoit que l'utilisateur soit informé de façon claire et complète sur les finalités du traitement, conformément à la Directive 95/46/CE. Le consentement peut, en principe, « être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée⁹¹. »

88) Voir Johannes Kuhn, « Provinzgekickte vor Millionen Zuschauern – Facebook entdeckt den Fußball », 18 août 2011, <http://www.sueddeutsche.de/digital/englische-pokalbegegnung-im-live-stream-facebook-sorgt-fuer-fussballrausch-in-der-provinz-1.1132389>

89) Sur ce point, Thomas Stadler, « Gilt deutsches Datenschutzrecht für Facebook überhaupt? », 18 août 2011, <http://www.internet-law.de/2011/08/gilt-deutsches-datenschutzrecht-fur-facebook-ueberhaupt.html>, estime que le droit allemand en matière de protection des données est applicable au traitement des données à caractère personnel des utilisateurs allemands par Facebook.

90) ULD, « Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook », 19 août 2011, disponible sur : <https://www.datenschutzzentrum.de/facebook/>

91) Voir considérant 17 de la Directive 2002/58/CE.

En ce qui concerne la mise en œuvre concrète de ces exigences, le CEPD suggère⁹² de permettre une déclaration de consentement par le biais des paramètres du navigateur, comme l'autorise de manière explicite le considérant 17 de la directive 2002/58/CE. Une solution appropriée devrait, de l'avis du CEPD, aussi être à la fois plus « conviviale *et* efficace. » La commissaire européenne chargée de la Stratégie numérique a vanté récemment le modèle « anti-traçage » (« *do-not-track* ») basé sur « le droit d'opposition » (*opt-out*) qui est mis en œuvre dans certains navigateurs récents.

Le CEPD a critiqué cette position et préconisé l'installation d'un « assistant de confidentialité » dans le logiciel de navigation pour s'assurer que l'utilisateur puisse régler les paramètres de confidentialité à sa guise avant utilisation. En outre, les paramètres par défaut devraient empêcher le stockage de cookies par des tiers, sauf si l'utilisateur en décide formellement autrement. Ce concept de « confidentialité par défaut » pourrait en principe trouver son application dans d'autres formes de publicité comportementale en ligne, qui ont recours à certaines configurations logicielles et matérielles (par exemple les décodeurs numériques ou les logiciels propriétaires).

IV. Perspectives

En principe, les individus peuvent accéder de plus en plus facilement aux médias publics. En particulier, l'internet a considérablement facilité la diffusion d'informations à un cercle de destinataires non connu à l'avance et virtuellement illimité. Aujourd'hui, la mise en place d'un média de masse (blogs, page Facebook), ne pose pas de véritable problème organisationnel, technique ou financier, grâce, en particulier, aux outils (gratuits pour la plupart) mis à disposition à cet effet. Grâce aux moteurs de recherche et autres outils, la possibilité de découvrir les informations mises en ligne ne dépend plus des institutions chargées d'agrégier les contenus, telles que les sociétés de presse et les radiodiffuseurs, qui fournissent à l'utilisateur une plateforme familière et lui facilitent ainsi la recherche des informations.

Traditionnellement, ces institutions ne se contentent pas de compiler des contenus (externes ou internes) et de les rendre accessibles. Elles se distinguent par le fait qu'elles endossent la responsabilité éditoriale des informations présentées. Dans le cadre du travail éditorial, qui englobe notamment la collecte, la vérification, l'appréciation, la classification, le traitement et l'organisation des données, elles sont soumises à des obligations légales ou d'autorégulation de diligence, tout en bénéficiant des droits spécifiques correspondants. La question se pose de savoir si on peut systématiquement présumer qu'un particulier qui publie également des contenus sur *Facebook* ou d'autres médias similaires est conscient de ces contraintes. Quoiqu'il en soit, on n'applique généralement pas le même niveau d'exigence aux obligations découlant de ses activités que pour les médias traditionnels.

Si, comme le demande la CJUE, les Etats membres optent pour une interprétation large des exemptions visées à l'article 9 de la Directive 95/46/CE en fonction des fins journalistiques du traitement de données, en principe, tout individu se livrant à une activité journaliste pourra bénéficier de ce privilège. Néanmoins, on peut douter que les pays européens parviennent à l'unanimité sur les dérogations à accorder au « prosommateur » individuel en matière d'obligations juridiques liées à la protection des données⁹³. Il semble qu'il manque (encore) des critères clairs pour structurer et définir le processus d'évaluation du droit à la protection des données à caractère personnel (et plus généralement de la personnalité) face à la liberté des médias. Ceci peut être lié aux différences culturelles entre les États membres : comme nous l'avons vu, d'une part, les pays scandinaves semblent avoir une appréciation sensiblement différente de l'Allemagne, entre autres, concernant le besoin de protection des données, telles que, par exemple, les données relatives aux

92) CEPD, *op. cit.* (note 86), p. 5 et s.

93) Voir au sujet du débat sur ce thème au Canada : <http://knightcenter.utexas.edu/blog/quebec-pushing-forward-controversial-proposal-define-professional-journalistsw>

revenus financiers⁹⁴. D'autre part, la conception de ce qu'est le journalisme est manifestement très hétérogène. Par conséquent, on est en droit de douter que la révision de la Directive 95/46/CE débouche sur une harmonisation renforcée de l'article 9.

Actuellement, on ignore encore si l'on continuera de ne considérer que celui qui est à l'origine de la diffusion de l'information, ou si l'on impliquera ceux qui donnent accès à ces informations par des moteurs de recherche ou des liens. Vont-ils également être considérés comme responsables et, si oui, quels seront leurs droits et leurs obligations ? Ce point implique une (nouvelle) mise à jour de la directive e-commerce, notamment sur les exonérations de responsabilités et l'instauration d'un juste équilibre avec le droit à la protection des données.

Comme nous l'avons exposé, les développements dans les nouveaux médias fournissent une occasion de traiter également la question de la protection des données à caractère personnel des utilisateurs. Outre les services proposés par les entreprises de médias professionnelles, ceci concerne également les offres que toute personne privée peut fournir - avec ou sans l'utilisation de plateformes professionnelles telles que YouTube ou Facebook. La question de la confidentialité comporte également plusieurs facettes. L'un des aspects essentiels est sans doute la « position de sandwich » dans laquelle se retrouve souvent tout prestataire non-professionnel : s'il utilise une plateforme professionnelle pour mettre à disposition ses contenus, cela engendre avec le fournisseur des rapports qui sont soumis à la protection des données. Dans le même temps, la protection des données à caractère personnel intervient également dans ses relations avec les utilisateurs des contenus publiés par ses soins. La question fondamentale concernant la nature de la responsabilité incombant au *prosommateur*, en particulier dans la seconde configuration, n'a pas encore trouvé de véritable réponse⁹⁵. La grande incertitude qui règne sur le niveau de connaissance du *prosommateur* concernant les processus de traitement des données internes à la plateforme, et sur sa capacité d'action éventuelle, joue, à cet égard, un rôle majeur

C'est donc avec beaucoup d'intérêt que l'on suivra les solutions qui seront proposées et retenues pour répondre aux nombreuses questions sur les médias et la protection des données, notamment dans le cadre de la révision des instruments juridiques de l'UE et du Conseil de l'Europe.

94) Le secret fiscal sous peine de sanctions (article 30 du Code des Impôts) permet la divulgation de renseignements fiscaux par les agents de la fonction publique uniquement dans quelques cas exceptionnels.

95) Dans le cas, tout au moins, où le *prosommateur* exploite également le site internet à partir duquel les contenus qu'il a produits sont mis à disposition, il est tenu - en tant que personne ayant accès aux systèmes techniques de traitement des données - de respecter vis-à-vis des utilisateurs de son « service de média » toutes les règles en matière de protection des données qui sont applicables au traitement des données en lien avec la prestation de service. Dans le cadre de la réglementation européenne, cela signifie, en bref, qu'il a besoin, pour traiter les données des utilisateurs, soit du consentement de la personne concernée, soit d'un fondement légal.