PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Manuel pour les journalistes

Auteurs: Iñigo de Miguel Beriain, Lorena Pérez Campillo (UPV/EHU)

Éditeur: Federico Caruso (OBC Transeuropa)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains This report is the property of the PANELFIT consortium and shall not be distributed or reproduced without the formal approval of the PANELFIT Project Coordinator.

Table des matières

1. Introduction

Le monde du journalisme est un microcosme très particulier en termes de protection des données. Même s'il implique la collecte et le stockage d'énormes quantités d'informations personnelles sous forme d'interviews, de dossiers d'entreprise, de photographies et de films, ainsi que leur diffusion, son cadre réglementaire n'a jamais été aussi clair. Ainsi, il n'est pas surprenant que lorsqu'il s'agit de l'activité des médias, il existe de sérieuses préoccupations liées à la protection des données (Erdos, 2015, p.8). En effet, la publication d'informations relatives à une personne identifiée ou identifiable pourrait constituer une atteinte grave à sa vie privée.

D'autre part, il est indéniable que le travail du journalisme est essentiel à la construction d'une opinion publique bien formée. En effet, les membres des médias sont souvent considérés comme des chiens de garde publics jouant un rôle essentiel dans une société démocratique. Ils ont le devoir de diffuser des informations et d'informer le public sur toutes les questions d'intérêt public, que le public a également le droit de recevoir (Lignes directrices sur la protection de la vie privée dans les médias, p.6). Ainsi, les médias ont le devoir de rapporter de manière adéquate les événements qui pourraient être d'intérêt public, même si cela peut mettre en danger les droits de certaines personnes affectées par leur publication.

Par conséquent, il existe deux droits fondamentaux, la liberté d'expression et la vie privée, qui entrent parfois en conflit. Cela soulève une question qui ne peut être résolue que par leur juste équilibre dans chaque cas concret. Quand le droit à la protection des données à caractère personnel prévaut-il sur le droit à la liberté d'expression et d'information et vice versa ? Il s'agit d'une question qui a déjà été étudiée en profondeur d'un point de vue juridique. Cependant, l'approbation du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, RGPD) et la protection renforcée des droits à la protection des

données ouvrent la porte à de nouveaux débats. Nous pensons que les journalistes et les organisations de médias de masse doivent être conscients de cette situation.

Le présent manuel n'a pas pour objectif de se concentrer sur les aspects théoriques de cette question, mais de fournir aux professionnels de l'information - journalistes, rédacteurs de l'information, directeurs des médias, etc. - des mécanismes adéquats pour garantir le respect des normes légales et éthiques minimales en matière de protection des données, tout en assurant un exercice adéquat de leur profession. Ce manuel s'adresse à toute personne travaillant dans une organisation médiatique, puisqu'elle peut bénéficier des exemptions ou des dérogations prévues par l'article 85.2 du GDPR.

Le contenu de ce manuel mélange plusieurs cadres réglementaires différents : d'une part, le règlement de l'UE, principalement le GDPR ; d'autre part, la réglementation du Conseil de l'Europe à travers la Convention européenne des droits de l'homme et la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Ces sources sont complétées par la jurisprudence de la CEDH et de la CJUE. Comme l'a déclaré le groupe de travail "Article 29", "un élément important qui ressort de la situation législative actuelle dans les États membres est que les médias, ou du moins la presse, sont tenus de respecter certaines règles qui, bien que ne faisant pas partie de la législation sur la protection des données au sens propre, contribuent à la protection de la vie privée des personnes. Cette législation et la jurisprudence souvent riche en la matière confèrent des formes de recours spécifiques qui sont parfois considérées comme un substitut à l'absence de recours préventifs prévus par la législation sur la protection des données" (A29WP, p. 7). Par conséquent, les orientations fournies dans le présent manuel sont destinées à suivre la réglementation fournie par toutes les institutions mentionnées..

Le manuel est divisé en plusieurs parties. Dans ses premières sections, il expose le cadre juridique relatif aux questions de journalisme et de protection des données dans l'UE. Les sections quatre et cinq, en revanche, se concentrent sur la manière de traiter les principales questions éthiques qui doivent être abordées par un journaliste ou une organisation médiatique dans le cadre du GDPR et des règlements du Conseil de l'Europe. Enfin, les annexes fournissent des informations détaillées sur le test de mise en balance et le cadre réglementaire au niveau des États membres.

CLAUSE DE NON-RESPONSABILITÉ: Ce document a pour but d'aider les journalistes à faire face au règlement sur la protection des données. Toutefois, son contenu ne constitue pas un avis juridique, n'est pas destiné à remplacer un avis juridique et ne doit pas être considéré comme tel. Vous devez solliciter un avis juridique ou un autre avis professionnel pour toute question particulière que vous ou votre organisation pourriez avoir.

2. Le cadre juridique de la liberté d'expression et de la protection des données dans l'UE

Le cadre réglementaire concernant le droit à la liberté d'expression et le régime de protection des données en Europe est principalement lié aux systèmes juridiques du Conseil de l'Europe et de l'Union européenne. Dans le cas du Conseil de l'Europe, la réglementation est double. D'une part, les principaux droits en jeu, le droit à la liberté d'expression et le droit à la vie privée, font partie de la Convention européenne des droits de l'homme. Son article 10.1 stipule que "Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans ingérence d'autorités publiques et sans considération de frontières. Le présent article n'empêche pas les États d'exiger l'octroi d'une licence aux entreprises de radiodiffusion, de télévision ou de cinéma". De toute évidence, ce droit pourrait être limité en vertu des dispositions du point 2 de cette clause. L'article 8, au contraire, se concentre sur la défense de la vie privée, en déclarant que :

> "1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence soit prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui".

D'autre part, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), également approuvée par le Conseil de l'Europe, régit les questions de protection des données. En effet, à l'heure actuelle, il s'agit du seul accord international juridiquement contraignant en matière de droit de la protection des données. Toutefois, la Cour européenne des droits de l'homme n'entend pas les affaires relatives aux violations présumées de cette convention, car elle est uniquement liée à la Convention européenne des droits de l'homme.

Dans le contexte de l'UE, le droit à la liberté d'expression a été inclus dans l'article 10 de la Charte des droits fondamentaux de l'UE, qui se lit comme suit :

> "1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.
>
> 2. La liberté et le pluralisme des médias sont respectés".

Au lieu de cela, les articles 7 et 8 de la Charte incluaient le droit à la vie privée et le droit à la protection des données personnelles le concernant. À l'heure actuelle, le cadre juridique de la protection des données est principalement dessiné par le règlement (UE) 2016/679 du GDPR. Les violations présumées de ce texte sont examinées par la Cour de justice de l'Union européenne (CJUE). Il n'existe aucun texte équivalent de droit dérivé global et complet sur la liberté d'expression et la liberté des médias principalement en raison de la position de la Commission selon laquelle l'UE n'est pas habilitée à légiférer dans ce domaine (Biriukova, 6).

Le GDPR s'applique dès lors que quiconque traite (collecte, conserve, utilise ou divulgue, par exemple) des informations concernant une personne vivante. Comme le fait remarquer l'ICO, "il n'empêche pas le journalisme responsable, car les grands principes sont suffisamment souples pour s'adapter aux pratiques journalistiques quotidiennes (...) Toutefois, les médias ne sont pas automatiquement exemptés et devront veiller à prendre en considération les droits des personnes en matière de protection des données. La responsabilité légale incombe généralement à l'organisation médiatique

concernée plutôt qu'aux employés individuels, bien que les journalistes indépendants soient susceptibles d'avoir leurs propres obligations distinctes". Toutefois, il est bon de toujours garder à l'esprit que les employés des organisations de médias doivent être conscients de leurs responsabilités légales, notamment en ce qui concerne le respect des règles au jour le jour, lorsqu'ils travaillent pour leur employeur.

3. L'"exemption journalistique" dans le GDPR

3.1 Introduction et contexte

Le GDPR est le principal outil juridique concernant les questions de protection des données au niveau de l'UE. Il contient les principes et règles généraux qui s'appliquent à tout traitement de données à caractère personnel au sein de l'UE ou impliquant des citoyens de l'UE. Au sein de ses dispositions, il est possible de trouver une référence spécifique aux questions en jeu. Nous parlons de ce que l'on appelle " l'exemption journalistique ", telle qu'énoncée par l'article 85 du GDPR, qui est présentée dans le tableau ci-dessous.

Cette clause a été incluse dans le GDPR comme une solution pour atténuer les tensions entre la liberté d'expression et le droit à la protection des données. En effet, elle visait à codifier la nécessité générale d'équilibrer ces deux droits fondamentaux. À première vue, elle a simplement laissé entre les mains des États membres la possibilité d'exempter ceux qui exercent leur liberté d'expression à des "fins journalistiques" des règles et obligations spécifiques du GDPR (Biriukova, 14).

Cette exemption journalistique n'était pas une nouveauté dans la réglementation de l'UE. L'article 9 de la directive sur la protection des données de 1995, le prédécesseur du GDPR, comprenait déjà une disposition similaire, ce qui a entraîné une certaine divergence dans la réglementation de cette question dans les États membres de l'UE. Une recommandation du groupe de travail "Article 29" a [1]résumé la situation en divisant les États membres en trois groupes principaux :

1 Toutefois, le groupe de travail a également indiqué que "les différences entre ces trois modèles ne doivent cependant pas être surestimées. Dans la plupart des cas, indépendamment de toute dérogation expresse pouvant exister, la législation sur la protection des données ne s'applique pas pleinement aux médias en raison du statut constitutionnel particulier des règles relatives à la liberté d'expression et à la liberté de la presse. Ces règles limitent de facto l'application des dispositions de fond en matière de protection des données ou du moins leur application effective. D'autre part, les données ordinaires". Voir :

"a) Dans certains cas, la législation sur la protection des données ne contient aucune exemption expresse de l'application de ses dispositions aux médias. C'est la situation actuelle en Belgique, en Espagne, au Portugal, en Suède et au Royaume-Uni.

b) Dans d'autres cas, les médias sont exemptés de l'application de plusieurs dispositions de la législation sur la protection des données. C'est la situation actuelle dans le cas de l'Allemagne, de la France, des Pays-Bas, de l'Autriche et de la Finlande. Des dérogations similaires sont envisagées par le projet de loi italien.

c) Dans d'autres cas, les médias sont exemptés de la législation générale sur la protection des données et régis par des dispositions spécifiques en la matière. C'est le cas au Danemark pour tous les médias et en Allemagne pour les radiodiffuseurs publics, qui ne sont pas couverts par les lois fédérales ou des Länder sur la protection des données, mais sont soumis à des dispositions spécifiques de protection des données dans les traités inter-Länder qui les réglementent".

Le GDPR n'a introduit que des changements mineurs dans ce scénario. En fait, l'article 85 du GDPR fournit un cadre d'action très large aux États membres. Ils doivent déterminer le champ d'application de l'exemption journalistique et les circonstances dans lesquelles elle s'applique. Toutefois, pour que leurs évolutions réglementaires soient valables, elles doivent être alignées sur les dispositions du GDPR et de la Convention européenne des droits de l'homme (CEDH). Il faut donc réfléchir aux règles à suivre dans l'environnement journalistique dans une double perspective. D'une part, il faut toujours garder à l'esprit une série de règles qui sont intégrées dans le GDPR et/ou la CEDH et la jurisprudence de la CJUE et de la CEDH. Celles-ci doivent être strictement suivies dans l'exercice de cette profession. D'autre part, il faut considérer qu'il peut y avoir certaines différences entre les États membres, en fonction du cadre réglementaire particulier. En tout état de cause, elles ne doivent pas être excessives puisque les principes et les règles du RGPD et de la CEDH doivent toujours être respectés.

Groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel, Droit de la protection des données et médias, Recommandation 1/97, p. 6-7, à l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf..

Néanmoins, il est important de souligner que certains États membres n'ont pas pleinement adhéré à ces normes. En Bulgarie, par exemple, la Cour constitutionnelle a récemment déclaré inconstitutionnelle l'approche nationale de la mise en œuvre de l'article 85. Cela était dû à l'inclusion d'un article dans la loi sur la protection des données personnelles qui énonçait 10 critères permettant de décider si les journalistes ont respecté l'équilibre entre le droit à l'information et celui à la protection des données personnelles. La Cour a considéré que ces critères étaient trop vagues et pouvaient créer un risque d'interprétations arbitraires, une circonstance qui ouvrait la voie à un pouvoir d'interprétation imprévisible de la Commission pour la protection des données, pas nécessairement dans l'intérêt du public en ce qui concerne l'information pluraliste sur les politiques et les activités du gouvernement[2].

En outre, en Roumanie, le régulateur de la protection des données a été critiqué pour avoir utilisé le GDPR pour faire taire les voix critiques dans les médias nationaux. En novembre 2018, un cas a été signalé en Roumanie qui pourrait bien servir à refléter la tension entre la protection des données et la liberté d'expression. Il était lié à un article sur un scandale de corruption impliquant un homme politique et sa relation étroite avec une entreprise faisant l'objet d'une enquête pour fraude, qui a été publié sur la page Facebook de Rise Project, basée à Bucarest. Quelque temps après la publication de l'article, l'autorité roumaine de protection des données (ANSPDCP) a envoyé une série de questions aux journalistes auteurs de l'article.

En théorie, cela était dû à la nécessité d'assurer un équilibre entre le droit à la protection des données personnelles, la liberté d'expression et le droit à l'information. L'autorité a estimé que les journalistes de Rise avaient violé le GDPR en publiant les vidéos, les photos et les documents - en substance, les données privées de citoyens roumains - pour appuyer les allégations des reporters. Les journalistes ont été invités à fournir des informations qui pourraient révéler les sources de l'article, sous l'annonce que s'ils ne coopéraient pas, ils pourraient devoir faire face à une pénalité allant jusqu'à 20 millions d'euros (Warner, 2019).

2 La Cour constitutionnelle de Bulgarie rejette la clause de la loi sur la protection des données, 17 novembre 2019, https://sofiaglobe.com/2019/11/17/bulgarias-constitutional-court-rejects-data-protection-law-clause-on-media/#:~:text=La%20Constitutionnelle%20de la Bulgarie%20a%20ruled,that%20of%20personal%20data%20protection..

Un groupe de douze organisations de défense des droits de l'homme et des médias a réagi à cette demande en envoyant une lettre ouverte à l'ANSPDCP qui demandait à l'ANSPDCP d'analyser soigneusement les cas de GDPR susceptibles de mettre en danger la liberté d'expression. Elle demandait également la mise en place d'un mécanisme urgent et transparent pour évaluer les réclamations impliquant des opérations de traitement de données à des fins journalistiques. Dans le même temps, seize ONG de défense des droits numériques ont envoyé une lettre au Conseil européen de la protection des données, avec l'ANSPDCP et la Commission européenne en copie, demandant que le GDPR ne soit pas détourné afin de menacer la liberté des médias en Roumanie (Benezic, 2018). Par la suite, certains députés européens à Bruxelles ont critiqué l'affaire contre le Projet Rise et ont contesté l'interprétation roumaine de l'application du GDPR. Enfin, tout cela a conduit à des avertissements de la part de la Commission européenne (Nielsen, 2018). Cependant, à l'heure actuelle, il est difficile de savoir ce qui pourrait finalement se passer, puisque l'affaire est actuellement en cours.

D'autres États membres ont toutefois adopté la position inverse. Par exemple, la Suède a estimé que l'article 85 du GDPR laissait aux États membres une plus grande marge de manœuvre pour les exemptions que la directive sur la protection des données, notamment parce qu'il n'exige pas que le traitement soit effectué "uniquement" à des fins journalistiques (une formulation qui figurait dans la directive). En outre, le gouvernement suédois a fait valoir que le considérant 153 du GDPR stipule que le concept de liberté d'expression doit être interprété de manière large. Sur cette base, la nouvelle loi sur la protection des données comprend des exemptions ou des dérogations plus larges que la loi sur les données personnelles de 1998 (McCullagh, 45).

3.2 Le champ d'application personnel de l'exemption

Que signifie "objectifs journalistiques" ? Que signifie le terme "journalisme" ? Il n'y a rien de semblable à une définition du journalisme dans le règlement, puisqu'elle a été supprimée des premiers projets du GDPR[3]. Certains États membres ont créé leurs

3 En effet, le projet se lit comme suit : "Les États membres devraient classer les activités comme "journalistiques" aux fins des exemptions et dérogations à prévoir dans le cadre du présent règlement si l'objet de ces activités est la divulgation au public d'informations, d'opinions ou d'idées, quel que soit le support utilisé pour les transmettre. Elles ne devraient pas être limitées aux entreprises de médias et peuvent être entreprises à des fins lucratives ou non lucratives" (Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à

propres définitions. La plupart d'entre elles sont assez ouvertes, à l'exception principale de l'Autriche, qui a réservé l'exemption exclusivement aux " entreprises de médias, aux services de médias et à leurs employés " (Cullagh, 2019, p.5).

Cependant, il semble assez clair que le GDPR opte pour un sens ouvert et inclusif du terme, qui pourrait être applicable même si la réglementation nationale ne le reflète pas. En effet, dans l'affaire Buivids[4], la CJUE a accepté que l'exception de journaliste soit applicable à un citoyen qui a publié un enregistrement vidéo sur Youtube, prouvant que l'objet de l'enregistrement et de sa publication était la divulgation d'informations, d'opinions ou d'idées au public. De même, dans l'affaire[5] Satamedia, la CJUE a jugé que les activités de collecte et de diffusion de données pouvaient également être considérées comme "journalistiques", si leur objectif était de divulguer au public des informations, des opinions ou des idées, quels que soient les moyens employés. Le fait que le responsable du traitement soit une organisation non médiatique à but lucratif a été considéré comme non pertinent pour ces objectifs.

On ne sait pas ce qui se passerait si une organisation autrichienne qui pourrait être considérée comme une entreprise de médias ou un service de médias mettait en œuvre l'une des dérogations ou exceptions prévues par l'article 85. D'une manière ou d'une autre, cela créerait un conflit entre la réglementation autrichienne et le GDPR, qui demande explicitement une large extension du concept de journalisme. À notre avis, il est probable que l'interprétation du GDPR prévaudra.

En gardant cela à l'esprit, il semble qu'une définition large du journalisme ait beaucoup plus de sens qu'une définition étroite. Natalija Bitiukova a écrit que "le journalisme fait référence à la production et à la distribution d'informations et de nouvelles à un nombre indéterminé de personnes dans la poursuite de l'intérêt public et la contribution au débat public" (Bitiukova, p.4). Sa formulation s'accorde parfaitement avec le GDPR, à notre avis.

---

caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM/2012/011, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52012PC0011).

4 CJUE, Sergejs Buivids c. Datu valsts inspekcija, C-345/17, 14 février 2019.

5 CJUE, Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, 16 décembre 2008.

Le journalisme doit donc être défini comme une activité qui couvre toute production sur les nouvelles, les affaires courantes, les affaires de consommation ou les sports[6]. En effet, l'exemption porte sur les informations traitées uniquement à des fins journalistiques. Le concept peut également inclure les éditeurs et rédacteurs de blogs ou de pages web sur Internet, car les commentaires faits sur ces plateformes doivent être considérés comme une manifestation de leur propre liberté d'expression. Bien entendu, cela ne signifie pas que chaque blog ou commentaire publié en ligne relèvera du journalisme, puisque certains blogueurs entendent simplement prendre part à des interactions sociales courantes ou à d'autres utilisations récréatives d'Internet. En outre, les moteurs de recherche sont expressément exclus du concept et donc de l'exception[7].

3.3 Traitement des données personnelles: le champ d'application matériel

Comme on l'a vu, l'article 85 précise que des exemptions ou des dérogations peuvent être applicables à toute personne qui vise à divulguer au public des informations, des opinions ou des idées. Cependant, quel type de données pourrait être considéré comme tel ? Quelles sont les données personnelles qui peuvent être traitées à des fins journalistiques sans avoir à se conformer au GDPR ? Là encore, il n'y a pas de réponse simple à cette question. En principe, les États membres ont leur mot à dire sur le champ d'application matériel de l'exemption pour les journalistes et leurs politiques ne sont pas toujours les mêmes. Par exemple, l'article 7 de la loi roumaine n° 190/2018, qui introduit des dérogations pour le traitement des données à caractère personnel à des fins journalistiques, ne propose que trois scénarios alternatifs dans lesquels les données à caractère personnel peuvent être traitées à des fins journalistiques [8]:

6 Selon l'ICO, "avec l'art et la littérature, nous considérons qu'elle est susceptible de couvrir tout ce qui est publié dans un journal ou un magazine, ou diffusé à la radio ou à la télévision - en d'autres termes, l'ensemble de la production de la presse écrite et audiovisuelle, à l'exception de la publicité payante (...).It would En a wide range of , into (, and and). bref, l'exemption peut potentiellement couvrir la quasi-totalité des informations collectées ou créées dans le cadre de la production quotidienne de la presse et des médias audiovisuels, ainsi que des organes d'information ou d'actualité en ligne comparables. Toutefois, les recettes publicitaires, la gestion immobilière, la dette financière, la diffusion ou les relations publiques ne sont généralement pas considérées comme du journalisme" (OIC, 29).

7 CJUE, Google SLSpain et Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, C-131/12, 13 May 2014, par. 81

8 Plainte adressée à la Commission européenne par l'Association pour la technologie et l'Internet (ApTI), 2018, à l'adresse suivante : https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

1) s'il s'agit de données à caractère personnel qui ont été clairement rendues publiques par la personne concernée ;

2) si les données à caractère personnel étaient étroitement liées à la qualité de personne publique de la personne concernée ; ou

3) si les données personnelles sont étroitement liées au caractère public des actes dans lesquels la personne concernée est impliquée. Si l'une de ces trois situations s'applique, le GDPR (à l'exception du chapitre sur les sanctions) est entièrement exclu de l'application.

Ces trois scénarios alternatifs sont extrêmement limités par rapport à la jurisprudence actuelle de la Cour européenne de justice et de la Cour européenne des droits de l'homme. Ces deux cours considèrent que plusieurs facteurs doivent être mis en balance avant une analyse, les plus importants étant la contribution à un débat d'intérêt public, d'une part, et l'atteinte à la vie privée des personnes concernées, d'autre part. Par conséquent, la loi roumaine ne semble pas effectuer une conciliation adéquate entre le droit à la protection des données personnelles et le droit à la liberté d'expression et d'information.

Le Royaume-Uni a adopté une approche totalement différente. Sa loi sur la protection des données de 2018 considère que l'exception du journaliste s'applique au traitement des données personnelles lorsque trois conditions cumulatives sont réunies :

- les données en question doivent être traitées en vue de la publication de matériel journalistique,
- le responsable du traitement des données doit raisonnablement penser que, compte tenu notamment de l'importance particulière de l'intérêt public pour la liberté d'expression, la publication serait dans l'intérêt public,
- et le responsable du traitement des données doit raisonnablement penser que l'application de la disposition du GDPR énumérée serait incompatible avec sa finalité journalistique.

Cette approche semble beaucoup plus conforme au cadre réglementaire.

3.4. La condition de l'exemption

Les exemptions ou dérogations prévues par l'article 85 ne sont applicables que "si elles sont nécessaires pour concilier le droit à la protection des données à caractère

personnel avec la liberté d'expression et d'information". Quand cette nécessité s'applique-t-elle ? Le considérant 153 apporte un éclairage précieux pour répondre à cette question:

> *Le droit des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, avec le droit à la protection des données à caractère personnel conformément au présent règlement. Le traitement de données à caractère personnel à des fins exclusivement journalistiques ou d'expression académique, artistique ou littéraire devrait faire l'objet de dérogations ou d'exemptions à certaines dispositions du présent règlement si cela est nécessaire pour concilier le droit à la protection des données à caractère personnel avec le droit à la liberté d'expression et d'information, tel que consacré par l'article 11 de la Charte. Cela devrait s'appliquer en particulier au traitement des données à caractère personnel dans le domaine audiovisuel et dans les archives d'actualités et les bibliothèques de presse. Par conséquent, les États membres devraient adopter des mesures législatives qui prévoient les exemptions et les dérogations nécessaires aux fins de l'équilibre de ces droits fondamentaux.*

Ainsi, le GDPR a la volonté d'assurer un équilibre adéquat entre la protection des données et le droit à la liberté d'expression et d'information, tel que consacré par l'article 11 de la Charte[9]. C'est pourquoi les *dérogations ou exemptions à certaines dispositions du GDPR* ne s'appliquent que *si elles sont nécessaires pour concilier le droit à la protection des données personnelles et le droit à la liberté d'expression et d'information*. Cette idée d'équilibrer les deux droits a été approuvée par la jurisprudence de la Cour européenne des droits de l'homme et de la CJUE, qui exige qu'une mise en balance soit effectuée au cas par cas chaque fois qu'il existe un conflit réel entre ces droits. Le point essentiel, cependant, est de savoir comment procéder pour ce faire. L'OIC indique que pour le faire de manière adéquate, les organisations doivent tenir compte de ce qui suit :

- l'intérêt général du public pour la liberté d'expression,

9 Article 11. Liberté d'expression et d'information

1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

2. La liberté et le pluralisme des médias sont respectés.

- tout intérêt public spécifique dans le domaine concerné,
- le niveau d'intrusion dans la vie privée d'un individu, y compris si l'histoire pourrait être poursuivie et publiée d'une manière moins intrusive, et
- le préjudice potentiel qui pourrait être causé aux individus. Les orientations existantes énoncées dans les codes de pratique du secteur peuvent aider les organisations à réfléchir à ce qui est dans l'intérêt du public[10].

Dans ce contexte, la notion d'intérêt public est particulièrement pertinente, selon la jurisprudence de la Cour de justice de l'UE ou de la Cour européenne des droits de l'homme, comme mentionné dans des affaires telles que Buivids[11] ou Satakunnan c. Finlande[12]. Cependant, elle est difficile à définir. En effet, la Cour européenne des droits de l'homme s'est historiquement abstenue de donner une définition de l'"intérêt public". Néanmoins, elle a déclaré, dans le cadre des affaires[13] Von Hannover, qu'"un premier critère essentiel est la contribution apportée par des photos ou des articles de presse à un débat d'intérêt général". Ainsi, il semble que cette notion couvre " le débat public, politique et historique, les questions liées aux politiciens, le comportement des fonctionnaires, les grandes entreprises, les gouvernements, les questions liées au crime. Cependant, d'autres sujets moins apparents peuvent également être considérés comme répondant à l'intérêt public ou général" (Biriukova, 21).

En résumé, certaines variables doivent être assurément présentes dans la définition de l'intérêt public, qui doit comporter "un élément de proportionnalité - il ne peut être dans l'intérêt public d'interférer de manière disproportionnée ou irréfléchie avec les droits fondamentaux d'une personne en matière de vie privée et de protection des données. Si la méthode d'enquête ou les détails à publier sont particulièrement intrusifs ou préjudiciables à une personne, un argument d'intérêt public plus fort et plus spécifique à chaque cas sera nécessaire pour le justifier, au-delà de l'intérêt public général de la liberté d'expression" (ICO, 33). En effet, l'intérêt public ne peut être réduit à la soif d'information du public sur la vie privée d'autrui ou au désir de sensationnalisme, voire de voyeurisme du lecteur, comme la publication de détails sur les activités sexuelles d'une personnalité publique. Si le seul but d'un article est de satisfaire la curiosité du lectorat à l'égard des détails de la vie privée d'une personne, il ne peut être considéré comme contribuant à un quelconque débat d'intérêt général

10 OIC, p. 34

11 CJUE, Sergejs Buivids c. Datu valsts inspekcija, C-345/17, 14 février 2019, par. 60-61.

12 CEDH, Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande, App no 931/13, 21 juillet 2015.

13 CourEDH, Von Hannover c. Allemagne (n° 2), App. n° 40660/08 et 60641/08, 7 février 2012, par. 109.

pour la société (Lignes directrices sur la protection de la vie privée dans les médias, 12). Par exemple, dans l'affaire Standard Verlags GmbH c. Autriche (n° 2), il a été jugé qu'un journal avait violé la vie privée des personnes concernées en publiant un article commentant des rumeurs selon lesquelles l'épouse du président autrichien de l'époque cherchait à divorcer et entretenait des contacts étroits avec un autre homme politique. Selon la Cour, les journalistes ne peuvent pas rapporter des ragots sans intérêt sur les mariages des hommes politiques. Les lignes directrices sur la protection de la vie privée dans les médias soulignent que "pour déterminer si une personne est une personnalité publique, il importe peu pour les journalistes de savoir si une certaine personne est effectivement connue du public. Les journalistes ne peuvent être limités par les affirmations des personnes concernées selon lesquelles elles ne sont pas réellement connues du public. Ce qui importe, c'est de savoir si la personne est entrée dans l'arène publique en participant à un débat public, en étant active dans un domaine d'intérêt public ou dans un débat public" (Lignes directrices sur la protection de la vie privée dans les médias, 12-20). Une série d'exemples de phrases produites par la Cour européenne des droits de l'homme et rassemblées dans les lignes directrices a été incorporée dans le tableau suivant (les références complètes sont incluses dans la section Sources d'information à la fin de ce manuel).

Ces considérations ouvrent la voie à un débat plus approfondi sur la manière de mettre en balance l'intérêt public et le droit à la vie privée. Ce point sera analysé dans la section du présent manuel consacrée à l'intérêt légitime en tant que fondement juridique du traitement des données à caractère personnel.

3.5 Le champ d'application matériel de l'exception

L'article 85 trace un large champ d'application pour les exceptions et les dérogations, puisqu'il mentionne le chapitre II (principes), le chapitre III (droits de la personne concernée), le chapitre IV (responsable du traitement et sous-traitant), le chapitre V (transfert de données à caractère personnel vers des pays tiers ou des organisations internationales), le chapitre VI (autorités de contrôle indépendantes), le chapitre VII (coopération et cohérence) et le chapitre IX (situations spécifiques de traitement des données). Par conséquent, les exceptions et les dérogations pourraient porter sur les *principes généraux, les droits de la personne concernée, du responsable du traitement et*

du sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou des organisations internationales, les autorités de contrôle indépendantes, la coopération et la cohérence, et les situations spécifiques de traitement des données.

Toutefois, il est essentiel de noter que ce large champ d'application ne s'appliquera pas nécessairement à tous les États membres de l'UE. La clause stipule explicitement que les États membres doivent prévoir des exemptions ou des dérogations, mais elle n'énumère pas ces exceptions. Elle déclare seulement qu'ils *doivent* concilier par la loi le droit à la protection des données à caractère personnel avec le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et d'expression académique, artistique ou littéraire.

Par conséquent, la décision concernant les mesures concrètes à adopter appartient aux États membres. Ils sont censés élaborer un tel cadre réglementaire et notifier à la Commission les dispositions adoptées en matière d'exemptions ou de dérogations et, sans délai, toute modification ultérieure de la loi ou tout amendement les concernant. À l'heure actuelle (novembre 2020), tous les États membres n'ont pas élaboré un tel cadre juridique. Dans l'annexe II, nous avons inclus des informations sur la réglementation incorporée par les Etats membres de l'UE, y compris les données dans lesquelles la modification a été introduite. Cependant, il se peut que certains pays aient modifié leur cadre juridique par la suite.

3.6 Réglementation applicable

D'une manière générale, les journalistes doivent essayer d'éviter d'envoyer des données personnelles en dehors de l'Espace économique européen (EEE) sans protection adéquate. Ce qui est considéré comme une "protection adéquate" dépendra "de la nature de l'information, de l'objectif du transfert et de la situation juridique à l'autre bout, entre autres choses". Ce principe n'empêchera pas la publication en ligne, même si celle-ci rend les informations disponibles en dehors de l'EEE. Si la publication est conforme au DPA à d'autres égards (ou si elle est exemptée parce qu'elle est dans l'intérêt public), il sera approprié de la publier dans le monde entier" (ICO, 26).

Que faire si les journalistes sont basés dans un État membre mais souhaitent publier des contenus dans d'autres pays ou dans l'espace web ? Le GDPR stipule que "lorsque ces

exemptions ou dérogations diffèrent d'un État membre à l'autre, le droit de l'État membre auquel le responsable du traitement est soumis devrait s'appliquer". Cela pourrait entraîner des conséquences étranges. Par exemple, il semble qu'une publication d'un éditeur (ou d'un blogueur) basé en Espagne pourrait bénéficier de règles relativement laxistes en matière de protection de la vie privée des "célébrités" dans ce pays, même si la publication en question serait interdite si elle était publiée par un éditeur français et même si la publication espagnole est facilement (et directement en ligne) accessible depuis la France. En outre, ils pourraient même bénéficier du fait d'être basés en Espagne même si la publication était en français et destinée à un public français. Cette brève suggestion sur la loi applicable est insuffisante pour l'environnement en ligne. À moins que cette question ne soit abordée plus spécifiquement dans le successeur de la directive "vie privée et communications électroniques", elle pourrait rendre l'environnement juridique de la liberté d'expression très flou, en particulier dans l'environnement numérique en ligne (EDRI, 51).

4. Le GDPR appliqué au journalisme

4.1 Le GDPR en quelques mots

Le GDPR vise à stimuler la création d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, au renforcement et à la convergence des économies au sein du marché intérieur, et au bien-être des personnes physiques (considérant 2). Elle vise à garantir un équilibre adéquat entre la protection des données et de la vie privée et certains autres droits fondamentaux, tels que la liberté d'expression, par exemple.

Le règlement est principalement axé sur le traitement des données à caractère personnel, c'est-à-dire "toute information concernant une personne vivante identifiable qui est (ou sera) stockée sur un ordinateur ou un autre dispositif numérique, ou classée dans un système de classement organisé où elle peut être facilement trouvée" (ICO, 2). Par conséquent, elle se concentre sur les données structurées qui révèlent des informations sur une personne vivante. Des notes manuscrites ne sont pas considérées comme des données personnelles, par exemple. Cependant, si quelqu'un transfère ces notes sur un ordinateur et les organise, elles deviendront des données personnelles.

De même, les informations anonymisées ne sont pas des données personnelles, mais elles ne doivent pas être confondues avec les informations pseudonymisées, c'est-à-dire les informations qui pourraient être liées à une personne (voir la conceptualisation ci-dessous). Les informations qui font référence à des personnes décédées ne sont pas non plus protégées par le GDPR, même si leur publication peut générer des problèmes liés au droit à l'honneur ou à l'image publique. D'autre part, le fait qu'une donnée soit publique ou privée ne change pas sa nature de donnée personnelle. Il peut toutefois avoir des conséquences sur la licéité de son traitement.

4.2 Les bases juridiques du traitement des données

En général, aucune donnée personnelle ne peut être traitée sans une base légale. L'article 6 du règlement énonce jusqu'à six motifs légaux de traitement légitime, à savoir:

1. la personne concernée a donné son consentement au traitement de ses données personnelles pour une ou plusieurs finalités spécifiques
2. le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures, à la demande de la personne concernée, préalables à la conclusion d'un contrat.
3. le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
4. le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique
5. le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
6. le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel, en particulier lorsque la personne concernée est un enfant.

Il existe trois bases juridiques pour le traitement qui s'appliquent généralement aux journalistes. Il s'agit du consentement, de l'intérêt public et de l'intérêt légitime. Elles seront examinées en détail dans la section 5.3.

4.3 Les catégories particulières de données

Certaines données sont spécialement protégées par le GDPR et les journalistes doivent être extrêmement prudents s'ils acceptent de les traiter. Ces catégories spéciales

comprennent : les données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Un responsable du traitement ne peut traiter ces données que s'il a un motif légal de procéder conformément à l'article 6 du GDPR et si l'une des circonstances qui atténuent l'interdiction introduite à leur traitement par l'article 9.1 s'applique. Ces circonstances sont énumérées à l'article 9.2 du GDPR. En principe, le consentement explicite du sujet qui fournit l'information ou la divulgation publique par les personnes auxquelles l'information se rapporte semblent les circonstances les plus prometteuses. Quoi qu'il en soit, le responsable du traitement doit toujours considérer que, comme ces types de données sont particulièrement sensibles, il ne doit les divulguer que si un intérêt public substantiel s'applique. Dans le tableau suivant, vous trouverez une compilation de la Cour européenne des droits de l'homme fournie par les Lignes directrices sur la protection de la vie privée dans les médias, qui rassemblent la jurisprudence de la Cour européenne des droits de l'homme.

À ce sujet, l'ICO a déclaré que "si les informations sont des "données personnelles sensibles", les organisations doivent également remplir l'une des conditions suivantes :

- la personne a donné son consentement explicite
- l'information a déjà été rendue publique à la suite de mesures qu'une personne a délibérément prises. Il ne suffit pas qu'elle soit déjà dans le domaine public - il faut que ce soit la personne concernée qui ait pris les mesures qui l'ont rendue publique" (ICO, 41).

4.4 Les droits du sujet et les devoirs du responsable du traitement

Enfin, il est essentiel de mentionner que le GDPR fournit aux personnes concernées certains droits essentiels qui doivent être respectés, sauf dérogations et exceptions applicables. Il s'agit notamment de :

- le droit d'accès. La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsque c'est le cas, l'accès aux données à caractère personnel et des informations concernant des questions telles que les finalités du traitement, les catégories de données à caractère personnel concernées, les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, etc. (voir article 15 du GDPR).
- Le droit de rectification. La personne concernée a le droit d'obtenir du responsable du traitement, sans retard excessif, la rectification de données à caractère personnel inexactes la concernant. Compte tenu des finalités du traitement, la personne concernée a le droit de faire compléter des données à caractère personnel incomplètes, y compris en fournissant une déclaration complémentaire.

- Droit à l'effacement ("droit à l'oubli"). La personne concernée a le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant sans retard excessif et le responsable du traitement a l'obligation d'effacer les données à caractère personnel sans retard excessif lorsque les circonstances énumérées à l'article 17 du GDPR s'appliquent.

- Droit à la limitation du traitement. La personne concernée a le droit d'obtenir du responsable du traitement la limitation du traitement lorsque l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une période permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ; ou le traitement est illicite et la personne concernée s'oppose à l'effacement des données à caractère personnel et demande à la place la limitation de leur utilisation ; ou le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement, mais elles sont requises par la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ; ou la personne concernée s'est opposée au traitement conformément à l'article 21, paragraphe 1, en attendant de vérifier si les motifs légitimes du responsable du traitement prévalent sur ceux de la personne concernée.
- Droit à la portabilité des données. La personne concernée a le droit de recevoir les données à caractère personnel la concernant, qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine.

En outre, le responsable du traitement doit s'acquitter de deux obligations essentielles selon le GDPR :

- obligation de fournir à la personne concernée des informations, qu'elles aient été collectées auprès d'elle ou non. Cela comprend des informations sur l'identité et

les coordonnées du responsable du traitement et, le cas échéant, de son représentant, les coordonnées du délégué à la protection des données, le cas échéant, les finalités du traitement auquel les données à caractère personnel sont destinées ainsi que la base juridique du traitement, etc. (voir articles 13 et 14 du RGPD).

- obligation de notification concernant la rectification ou l'effacement des données à caractère personnel ou la limitation du traitement. Le responsable du traitement communique toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement à chaque destinataire auquel les données à caractère personnel ont été divulguées, sauf si cela s'avère impossible ou implique des efforts disproportionnés. Le responsable du traitement informe la personne concernée de ces destinataires si celle-ci le demande.

4.5 Les principaux concepts

Plusieurs concepts sont particulièrement pertinents dans le contexte du GDPR et les journalistes doivent être conscients de leur signification. Il s'agit de :

- «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

- «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utili- sation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rappro- chement ou l'interconnexion, la limitation, l'effacement ou la destruction

- La «pseudonymisation» désigne le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisa- tionnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

- «fichier», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

- Le «responsable du traitement» est la la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre..

- Le «sous-traitant» est une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

- Le terme «destinataire» désigne une personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

- «tiers», une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel

- Le «consentement» de la personne concernée est toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

5. Les principes appliqués au journalisme

5.1 Introduction

Cette section vise à fournir aux journalistes quelques conseils concrets pour faire face à leurs activités quotidiennes. Elle utilise un langage simple et facile à comprendre, qui peut être compris par un non-expert. Elle est structurée sur la base des principes fixés par le GDPR. Cela est dû à un fait simple : le traitement doit toujours respecter ces principes, qui sont au cœur du GDPR. Cela signifie que même si vous avez un motif légal

pour traiter des données personnelles, vous devez respecter ces principes fondamentaux. Dans le cas contraire, votre traitement ne serait pas licite.

Dans les pages suivantes, nous montrons ces principes et fournissons des conseils sur la manière de les traiter du point de vue d'un journaliste. Ces conseils intègrent les recommandations formulées par le Conseil de l'Europe dans ses Lignes directrices sur la sauvegarde de la vie privée dans les médias approuvées conjointement en juin 2018 par le Comité directeur sur les médias et la société de l'information (CDMSI) et le Comité de la Convention 108 (Convention sur la protection des données du Conseil de l'Europe). Ces Lignes directrices comprennent un ensemble de normes du Conseil de l'Europe (le Conseil/CoE) et de la Cour européenne des droits de l'homme (la Cour) concernant la protection de la vie privée des personnalités publiques et des personnes privées dans les médias. **Veuillez toujours garder à l'esprit que cette partie du Manuel fournit principalement des conseils sur la manière de traiter les principes adoptés par le GDPR d'un point de vue éthique. Afin d'assurer une conformité juridique adéquate, vous devez suivre la réglementation produite par l'État membre correspondant.**

5.2 Légalité, équité et transparence

Selon l'article 5.1 (a) du GDPR, " Les données à caractère personnel sont traitées de manière licite, loyale et transparente à l'égard de la personne concernée ". Ce principe comprend trois exigences différentes.

- Légitimité. Le traitement des données n'est licite que si une base de légitimité le permet (voir section 3.1). La plupart des informations qu'un journaliste collecte sont des données personnelles. Ainsi, l'obtention d'informations implique souvent le traitement de données et, par conséquent, doit suivre les principes établis par le GDPR. Cela signifie que vous devez avoir une base légale pour traiter les données et que vous devez justifier les raisons pour lesquelles vous les collectez.

- L'équité. Le concept de loyauté est difficile à définir. Elle renvoie au fait que le traitement doit être conforme à l'esprit du RGPD, et pas seulement à sa lettre. Il permet ainsi d'introduire dans l'application du RGPD les dispositions d'autres réglementations particulièrement importantes lorsqu'il s'agit de définir ce qui est considéré comme " équitable " au sein de l'UE et de ses États membres, comme la Charte des droits fondamentaux de l'UE. En général, cependant, on pourrait affirmer que la loyauté implique que vous traitiez les informations

d'une manière qui satisfasse les attentes rationnelles des personnes concernées. L'ICO a déclaré que la loyauté signifie que "dans la mesure du possible, les médias doivent collecter et utiliser les informations sur les personnes de manière loyale et légale, et ne pas causer de préjudice injustifié". Les journalistes pourront souvent recueillir des informations à l'insu du sujet ou sans son consentement, mais il sera injuste de tromper activement les gens sur l'identité ou les intentions du journaliste" (ICO, 40).

- La transparence. Le principe de transparence vise à garantir que toutes les parties intéressées sont conscientes de chaque traitement de leurs données personnelles et qu'elles peuvent accéder aux informations essentielles sur leur contenu spécifique. En général, vous devez également dire à la personne auprès de laquelle vous recueillez les informations, et à la personne sur laquelle portent les informations (c'est-à-dire la personne concernée), qui vous êtes et ce que vous faites de ses informations. Si elle vous fournit les informations dans un but précis, vous ne devez pas les utiliser dans un autre but. Parfois, le fait d'informer les personnes concernées du traitement des données pourrait nuire à l'activité journalistique. Parfois, vous utilisez des méthodes secrètes intrusives pour obtenir un article, comme la surveillance. Toutes ces circonstances peuvent être acceptables, pour autant que vous n'ayez pas d'autre solution plus conforme aux principes de la protection des données et que l'article soit d'intérêt public. En fait, c'est là le point essentiel : vous pouvez éviter de notifier le traitement à la personne concernée si et seulement dans la mesure où cela rendrait l'exercice du journalisme impossible. En d'autres termes, vous devez communiquer le traitement aux personnes concernées, sauf si vous considérez que, ce faisant, vous ne pourriez pas construire l'histoire. Une fois que cela ne s'applique plus, vous devez procéder aux obligations réglées par le GDPR. Comme l'a déclaré l'ICO, "dans le contexte du journalisme, nous acceptons qu'il ne sera généralement pas possible pour les journalistes de prendre contact avec toutes les personnes au sujet desquelles ils recueillent des informations. Il sera souvent juste de recueillir des informations sur des sujets d'intérêt journalistique potentiel à l'insu du sujet. Cependant, il y aura des cas où l'équité exigera un contact direct avec le sujet d'une enquête majeure, afin de lui offrir l'opportunité de présenter sa version de l'histoire" (ICO, 40).

5.3 Choix de la base juridique du traitement

Il existe trois bases juridiques pour le traitement qui s'appliquent généralement au journalisme. Il s'agit du consentement, de l'intérêt public et de l'intérêt légitime.

Consentement. Les données peuvent être traitées si les personnes qui font l'objet de l'information ont donné leur consentement. Si l'information concerne plusieurs personnes, le consentement doit être donné par toutes ces personnes. Le consentement doit être libre, spécifique et éclairé. Il faut souligner que le simple fait qu'une personne

ait publié des données personnelles sur un site public, comme son profil Facebook, ne signifie pas que ces données peuvent être utilisées sans son consentement ou une autre base juridique. Le consentement doit couvrir les finalités du traitement des données. Par conséquent, si vous souhaitez utiliser les données pour une finalité autre que celle initialement recherchée par la personne concernée, vous devez disposer d'une base juridique. Il peut y avoir des exceptions à cette règle, notamment si la personne concernée est une personnalité publique mais, dans ce cas, vous devez traiter les données sur la base de l'intérêt légitime, au lieu du consentement. Selon les Lignes directrices sur la protection de la vie privée dans les médias, "les journalistes devraient, en principe, obtenir le consentement de la personne concernée au moment où la photo est prise et pas seulement si et quand elle est publiée. Sinon, un attribut essentiel de la personnalité (l'image) dépend de tiers et la personne concernée n'en a pas le contrôle" (p. 20).

Intérêt public. Les données peuvent être traitées si elles sont nécessaires à l'exécution d'une tâche effectuée dans l'intérêt public. En effet, il s'agit de la base juridique la plus recommandable si vous faites partie d'une institution publique qui agit en tant que telle (si le consentement n'est pas applicable). Si vous êtes un acteur privé ou si vous êtes une institution publique qui travaille comme un acteur privé, la base de l'intérêt légitime est plus recommandable. Cela est dû au fait que l'intérêt public ne peut pas légitimer le traitement si nous ne tenons pas compte des intérêts de la personne concernée, car l'information n'est pas un droit ou un devoir absolu. Toutefois, si tel est le cas, l'intérêt légitime et le critère de mise en balance sont des concepts qui fonctionnent très bien avec le traitement. Il est donc recommandé d'utiliser l'intérêt légitime comme base juridique du traitement.

Intérêt légitime. Le traitement est nécessaire pour des "intérêts légitimes", à condition qu'il ne cause pas de préjudice injustifié à la personne concernée. "Les intérêts légitimes comprendront les intérêts commerciaux et journalistiques d'une organisation médiatique dans la collecte et la publication de matériel, ainsi que l'intérêt public dans la liberté d'expression et le droit de savoir". Il s'agit donc d'une base juridique large qui comprend l'intérêt public mais pas seulement. Afin d'équilibrer tous les intérêts en jeu, vous devez suivre une procédure capable de garantir que l'intérêt légitime sert de base juridique au traitement, qui comprend trois phases principales (Detrekői) :

- d'abord, vous devez identifier un test d'intérêt légitime (pourquoi l'histoire sert l'intérêt public)
- deuxièmement, vous devez effectuer un test de nécessité (comment la publication des noms et des données personnelles est nécessaire pour rendre l'article informatif)
- enfin, vous devez procéder à un test d'équilibre visant à démontrer que l'intérêt du public à connaître le sujet traité dans l'article dépasse l'intérêt de la personne à garder ses données personnelles cachées aux yeux du public. Plus la valeur de l'information pour le public est grande, plus l'intérêt d'une personne à être protégée contre la publication doit céder, et vice versa (Lignes directrices sur la protection de la vie privée dans les médias, p.11).

Une description détaillée d'un test de mise en balance figure à l'annexe I du présent document. La jurisprudence de la Cour européenne des droits de l'homme est très complète en ce qui concerne l'équilibre entre l'intérêt public et la vie privée (voir Droit à la protection de l'image, à l'adresse : https://www.echr.coe.int/documents/fs_own_image_eng.pdf). Un excellent résumé de sa position a été inclus dans l'affaire Kaboğlu et Oran c. Turquie : "Dans plusieurs de ses arrêts, la Cour a résumé comme suit les critères pertinents pour la mise en balance du droit au respect de la vie privée et du droit à la liberté d'expression : la contribution à un débat d'intérêt public, la notoriété de l'intéressé, le sujet du reportage, le comportement antérieur de l'intéressé, le contenu, la forme et les conséquences de la publication, ainsi que, le cas échéant, les circonstances de l'espèce (voir *Von Hannover* (no 2) [GC], précité, §§ 108-113, et *Axel Springer AG*, précité, §§ 89-95 ; voir également *Couderc et Hachette Filipacchi Associés*, précité, § 93). Si les deux droits en question ont été mis en balance d'une manière conforme aux critères établis par la jurisprudence de la Cour, celle-ci aurait besoin de raisons fortes pour substituer son point de vue à celui des juridictions internes (voir *Palomo Sánchez et autres c. Espagne* [GC], nos 28955/06, 28957/06, 28959/06 et 28964/06, § 57, CEDH 2011) ".

5.4 Limitation de l'objet

Les données à caractère personnel sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. En vertu de cela, les données ne peuvent être traitées que pour certaines finalités, qui doivent être explicitement indiquées lors de la justification du traitement. Par conséquent, vous devez toujours garder à l'esprit, par exemple, que vous

ne pouvez pas utiliser les données que vous conservez dans vos dossiers à des fins autres que celles qui ont justifié leur traitement, à moins que vous ne disposiez d'une base servant à justifier le nouveau traitement.

5.5 Minimisation des données

Les données à caractère personnel doivent être "adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées". Ce principe implique que "vous devez disposer de suffisamment d'informations pour faire le travail, mais ne devez pas disposer de ce dont vous n'avez vraiment pas besoin". Notez que ce principe tient compte de votre finalité. Comme la nature du journalisme exige la collecte et le recoupement de grands volumes d'informations, nous acceptons que des informations sans pertinence immédiate pour une histoire en cours puissent être conservées de manière justifiée pour une utilisation future si elles concernent une personne ou un sujet d'intérêt journalistique plus général" (ICO, 25).

5.6 Précision

Selon l'article 5.1(d), "les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel inexactes, au regard des finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai".

L'exactitude est à la fois un principe essentiel du GDPR et une valeur clé du journalisme. Par conséquent, les journalistes doivent veiller tout particulièrement à ce que les informations publiées soient exactes. À cette fin, il faut vérifier les faits. On peut faire valoir que seules des informations exactes fonctionnent bien avec l'idée de promouvoir l'intérêt public. Par conséquent, les exemptions et dérogations prévues par l'article 85 ne s'appliqueront que si l'information est exacte. "Toutefois, l'exemption peut être utilisée si, par exemple, l'histoire est urgente dans l'intérêt public et que le délai court rend très difficile une vérification complète de l'exactitude. Comme pour tout recours à l'exemption, vous devrez toujours démontrer qu'une personne d'un niveau approprié a réfléchi aux vérifications possibles, à la possibilité de retarder la publication pour

effectuer des vérifications supplémentaires, à la nature de l'intérêt public en jeu et que la décision de publier était, par conséquent, raisonnable" (ICO, 14).

En outre, l'exactitude implique que des mesures très raisonnables soient prises pour garantir que les données à caractère personnel qui sont inexactes soient effacées ou rectifiées sans délai. C'est essentiel, car les informations publiées peuvent compromettre gravement l'image publique ou la vie privée d'une personne. Selon l'article 29 WP, "le droit de réponse et la possibilité de faire rectifier des informations fausses, les obligations professionnelles des journalistes et les procédures spéciales d'autorégulation qui leur sont attachées, ainsi que le droit protégeant l'honneur (dispositions pénales et civiles concernant la diffamation) doivent être pris en considération lors de l'évaluation de la manière dont la vie privée est protégée en relation avec les médias" (A29WP, p. 7).

Les journalistes doivent donc être particulièrement prudents et modifier les informations s'il s'avère qu'elles ne reflètent pas fidèlement la réalité. Ceci, bien sûr, doit être particulièrement considéré si les personnes demandant la rectification sont les personnes concernées, conformément à leur droit de rectification. Enfin, vous devez toujours indiquer si vous exprimez une opinion ou si vous informez d'un fait. C'est essentiel pour que le public n'interprète pas mal l'information.

5.6 Limitation du stockage

Le principe de limitation de la conservation signifie que les données sont "conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées" (article 5 du GDPR). Dans le contexte du journalisme, cela signifie qu'une fois que vous avez vos informations, vous devez prendre certaines décisions quant à savoir si vous souhaitez les stocker et pour combien de temps. Les données sont des atouts très précieux pour les journalistes, car elles peuvent souvent servir de matériel de référence. Les coordonnées sont également une ressource très importante et les journalistes souhaitent généralement les conserver. En principe, vous pouvez conserver ces données pendant de longues périodes ou indéfiniment. Le GDPR n'impose pas de limite temporelle à la durée de conservation des données personnelles. Le principe de

"limitation de la conservation" impose seulement qu'il y ait une bonne raison de conserver les données. En supposant que ce soit le cas, elles peuvent être conservées indéfiniment.

Cependant, comme l'indique l'ICO (ICO, 12), "vous devriez revoir de temps en temps les informations que vous conservez pour vous assurer que les détails sont toujours à jour, pertinents et non excessifs par rapport à vos besoins, et vous devriez supprimer tous les détails dont vous n'avez plus besoin (par exemple, si un contact a changé de numéro). En outre, la manière dont vous conservez les informations ou dont vous les révisez doit être définie dans des politiques organisationnelles.

5.7 Intégrité et confidentialité

Les données doivent être " traitées d'une manière qui garantit une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dommages accidentels, au moyen de mesures techniques ou organisationnelles appropriées " (art. 5 GDPR). Ce principe vise à éviter les traitements non autorisés ou illicites et les pertes, destructions ou dommages accidentels des données.

Les données que vous stockez sont des éléments sensibles. Vous devez donc faire de votre mieux pour éviter qu'elles ne soient perdues, volées ou mal utilisées. Essayez de les garder en sécurité en prêtant attention aux procédures et aux protocoles de sécurité établis par votre organisation. En effet, tous les employés d'une entreprise de médias doivent connaître et suivre les politiques et procédures de l'organisation. Les informations doivent être verrouillées, protégées par un mot de passe et cryptées dans la mesure du possible. Vous devez être particulièrement attentif à la sécurité lorsque vous sortez du bureau avec des documents, des téléphones ou des ordinateurs portables contenant des données personnelles.

L'éventail des mesures de sécurité nécessaires n'est pas fixé. En principe, des mesures de sécurité peuvent être appropriées pour garantir qu'aucun accès illicite ne se produise ou pour éviter toute perte, destruction ou dommage accidentel. Les journalistes doivent prendre en considération le caractère sensible ou confidentiel des informations qu'ils détiennent, le préjudice qui pourrait résulter de leur perte ou de leur

utilisation abusive, la technologie disponible et les coûts impliqués. Ils ne sont pas obligés de disposer d'une sécurité de pointe, mais celle-ci doit être adaptée au niveau de risque. Les organisations doivent envisager des mesures de sécurité techniques (électroniques) et physiques, des politiques et des procédures, ainsi que la formation et la supervision du personnel. Ces mesures doivent couvrir le personnel travaillant à l'intérieur et à l'extérieur du bureau. Dans tous les cas, les organisations doivent être en mesure de justifier le niveau de sécurité adopté (ICO, 43).

5.8 Responsabilité

Selon l'article 5.2 du GDPR, "Le responsable du traitement est responsable du respect du paragraphe 1 et doit être en mesure de le démontrer". Cette clause stipule que le responsable du traitement est non seulement responsable de la conformité au GDPR, mais qu'il doit également être en mesure de démontrer cette conformité. Par conséquent, le responsable du traitement supporte la charge de la preuve de la conformité au GDPR. Dans le cas du journalisme, il peut arriver qu'en fait, une exemption aux droits du sujet ait été mise en œuvre. Dans ce cas, les organisations ou les journalistes doivent être en mesure d'expliquer pourquoi le respect des dispositions pertinentes n'était pas compatible avec les objectifs du journalisme. À cette fin, ils doivent souvent démontrer qu'ils ont effectué un test d'équilibre, en considérant les différents intérêts en jeu. Affirmer que la conformité n'est pas une pratique courante dans le secteur ne serait en aucun cas suffisant. Conserver une piste d'audit dans les cas qui sont controversés ou particulièrement susceptibles de l'être pourrait être un outil approprié pour démontrer la responsabilité.

Comme l'a déclaré Mme Biriukova, "premièrement, l'entreprise de presse, un journaliste ou toute autre personne souhaitant se prévaloir de l'exemption doit établir l'intérêt public de la publication envisagée et, deuxièmement, comprendre quelles obligations en matière de protection des données seraient, dans ce cas, en conflit avec les objectifs journalistiques". S'il est vrai que, dans le cas d'une enquête journalistique sur la corruption gouvernementale, le refus de divulguer la source de l'information pourrait être facilement défendu, d'autres scénarios, moins noirs et blancs (par exemple, les notifications de violation), pourraient créer des problèmes de conformité. En même temps, il est difficile de concevoir que, par exemple, un journaliste citoyen se livre a

priori à un tel exercice d'équilibrage. À moins que des orientations plus détaillées, des codes de pratiques ou de conduite ne soient fournis, une telle approche nuancée risque de rester largement théorique et non opérationnelle" (Biriukova, 22).

Il faut également toujours garder à l'esprit qu'en général, le responsable du traitement des données n'est pas un journaliste isolé, mais l'organisation dans laquelle il travaille. Par conséquent, l'organisation est responsable de la mise en œuvre de mesures et de politiques organisationnelles concernant le traitement des données et la responsabilité. En effet, l'organisation doit être en mesure de prouver que le traitement des données est le résultat final d'un processus décisionnel qui a pris en compte toutes les questions en jeu. Les procédures peuvent varier considérablement, en fonction du type d'organisation et d'information, mais il devrait y avoir une sorte de procédure structurée dans chaque organisation. En outre, il serait bon de développer certains codes de conduite dans le cadre de la profession de journaliste dans chaque État membre. En effet, le groupe de travail Article 29 a déclaré que "pour évaluer si les exemptions ou les dérogations sont proportionnées, il faut tenir compte des obligations éthiques et professionnelles existantes des journalistes ainsi que des formes d'autorégulation de la profession" (A29WP, p.8).

Comme l'indique l'ICO, "dans de nombreuses histoires quotidiennes, il peut être approprié pour le journaliste d'utiliser son propre jugement, mais les histoires plus médiatisées, intrusives ou préjudiciables sont susceptibles de nécessiter une plus grande implication de la rédaction et une considération plus formelle de l'intérêt public. Les politiques organisationnelles devraient être utilisées pour expliquer quand une plus grande implication de la rédaction est requise. Selon nous, c'est la conviction au moment du traitement qui est importante. Le responsable du traitement doit être en mesure de démontrer qu'il était convaincu de l'intérêt public, c'est-à-dire que la question de l'intérêt public a effectivement été prise en considération. Il doit également être en mesure de montrer qu'elle a été prise en considération au moment du traitement pertinent des données à caractère personnel et pas seulement après coup. Si un journaliste considère initialement qu'un article sera d'intérêt public, mais que l'organisation décide finalement de ne pas le publier, l'exemption peut toujours couvrir toutes les activités journalistiques entreprises jusqu'à ce moment-là.

Deuxièmement, l'exemption ne requiert qu'une croyance raisonnable. Cela donne beaucoup plus de marge de manœuvre que d'autres exemptions et reflète l'importance d'un média libre et indépendant (ICO, 35). Le tableau suivant présente certaines mesures incluses dans les Guidelines on Safeguarding Privacy in the Media qui pourraient être utiles aux organisations cherchant à assurer la conformité avec la protection des données.

6. Questions supplémentaires

6.1 Demandes d'accès des personnes concernées

L'accès aux informations stockées par les journalistes peut être très important, tant pour les sujets qu'ils couvrent que pour les autres personnes. Les premiers disposent toutefois d'un droit d'accès que les autres n'ont pas. L'article 85 permet toutefois aux États membres de limiter ce droit. Dans cette section, nous présenterons quelques considérations sur la manière dont cette limitation est généralement formulée. Ce faisant, nous nous concentrerons à la fois sur le droit d'accès et sur le droit de ne pas divulguer les sources d'information, qui sont largement reconnus en Europe.

Conformément à l'article 15 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsque c'est le cas, l'accès aux données à caractère personnel et aux informations concernant les finalités du traitement, les catégories de données concernées, les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, notamment les destinataires situés dans des pays tiers ou des organisations internationales, la durée envisagée de conservation des données à caractère personnel, etc.

Sur cette base, un journaliste devrait fournir aux personnes concernées les informations qu'il détient à leur sujet, à moins qu'il ne considère que, ce faisant, il ne serait pas en mesure de construire l'histoire. Dans ces circonstances, les exceptions et dérogations de l'article 85 prévaudraient sur leur droit d'accès. Il va sans dire que cela ne se produirait que dans l'hypothèse où l'histoire présente un intérêt public. Plus l'intérêt est élevé, plus le droit de ne pas divulguer les informations à la personne concernée est fort. Très

souvent, il peut arriver que vous puissiez donner accès à certaines informations sur le traitement ou les données à caractère personnel utilisées sans nuire aux objectifs de votre enquête. Si tel est le cas, vous devez procéder sans délai.

Le refus de fournir les informations demandées pourrait parfaitement se justifier même après la publication de l'article. Si vous avez de fortes raisons de considérer que cela pourrait être contraire à l'intérêt public, si vous êtes en mesure d'expliquer pourquoi répondre à la demande nuirait à de futures enquêtes ou publications, ou plus généralement aux activités journalistiques, vous pourriez refuser la demande. Mais vous devrez toujours donner une bonne raison de vous y opposer. Enfin, n'oubliez pas que vous ne devez pas inclure d'informations sur d'autres personnes à moins qu'elles n'aient donné leur consentement ou qu'il soit raisonnable de les fournir sans leur consentement.

6.2 Sources confidentielles

Les sources d'information sont sacrées pour les journalistes. Plusieurs instruments internationaux garantissent leur protection adéquate, notamment la Résolution sur les libertés journalistiques et les droits de l'homme, adoptée lors de la 4eth Conférence ministérielle européenne sur la politique des communications de masse (Prague, 7-8 décembre 1994) et la Résolution sur la confidentialité des sources des journalistes adoptée par le Parlement européen (18 janvier 1994, Journal officiel des Communautés européennes n° C 44/34). En outre, la recommandation n° R(2000) 7 sur le droit des journalistes de ne pas divulguer leurs sources d'information a été adoptée par le Comité des ministres du Conseil de l'Europe le 8 mars 2000. En outre, en général, le droit et la pratique internes des États membres prévoient une protection explicite et claire du droit des journalistes de ne pas divulguer des informations permettant d'identifier une source, conformément à l'article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Il existe donc un cadre juridique qui permet aux journalistes de ne pas divulguer leurs sources. Ce droit ne peut être limité que dans les conditions mentionnées par le principe 3(b) de la Recommandation n° R(2000) 7, à savoir :

"i. des mesures alternatives raisonnables à la divulgation n'existent pas ou ont été épuisées par les personnes ou les autorités publiques qui demandent la divulgation, et

ii. l'intérêt légitime de la divulgation l'emporte clairement sur l'intérêt public de la non-divulgation, en tenant compte des éléments suivants :

-une exigence impérieuse de la nécessité de la divulgation est prouvée,

-les circonstances sont d'une nature suffisamment vitale et sérieuse,

-la nécessité de la divulgation est identifiée comme répondant à un besoin social urgent, et

-Les États membres disposent d'une certaine marge d'appréciation pour évaluer cette nécessité, mais cette marge va de pair avec le contrôle de la Cour européenne des droits de l'homme.

c.Les exigences ci-dessus devraient être appliquées à tous les stades de toute procédure où le droit de non-divulgation pourrait être invoqué".

Enfin, il ne faut pas oublier que la révélation d'une source implique également un traitement des données. Et que la source est également une personne concernée qui dispose des droits conférés par le GDPR. Par conséquent, si la source est un individu, vous pourrez probablement préserver son identité sur la base du GDPR. En effet, si le sujet d'un reportage fait une demande d'accès et que celle-ci ne pourrait être satisfaite qu'en divulguant l'identité de vos sources, vous ne pourrez procéder que si la source y consent, ou s'il est raisonnable de le faire, toutes circonstances confondues. Si la source est une organisation, les circonstances changent puisque les organisations ne possèdent pas de données personnelles. Les journalistes doivent donc s'appuyer sur l'exception journalistique pour ne pas divulguer l'identité de la source si celle-ci n'est pas disposée à révéler son nom ou s'il n'est pas approprié de le faire.

6.3 Mineurs et population vulnérable

Vous devez être particulièrement prudent si vous êtes prêt à traiter des données concernant des mineurs ou des populations vulnérables. Premièrement, la base

juridique de ce traitement peut être faible. Le consentement d'un mineur ne sera valable que si ce dernier peut le donner conformément au cadre juridique de l'État membre. Le GDPR fixe un âge minimum, mais les États membres sont habilités à le relever. Par conséquent, vous devez vous informer à ce sujet. Si le mineur ou la personne vulnérable n'est pas en mesure de donner son consentement, ses représentants légaux doivent le faire.

Si vous ne pouvez pas obtenir un consentement éclairé, le traitement doit alors être fondé sur la base de l'intérêt légitime. Toutefois, l'intérêt légitime poursuivi par le responsable du traitement ne s'applique pas "lorsque des intérêts ou des droits et libertés fondamentaux de la personne concernée l'emportent sur les intérêts ou les droits et libertés fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, en particulier lorsque la personne concernée est un enfant". Par conséquent, il est hautement improbable que le test de mise en balance permette le traitement de données à caractère personnel correspondant à des mineurs. A notre avis, des réflexions similaires sont applicables aux populations vulnérables.

Les lignes directrices sur la protection de la vie privée dans les médias comprennent un résumé de deux affaires concernant des mineurs.

- " Dans l'affaire Kahn c. Allemagne, des photos de deux enfants d'Oliver Kahn, ancien gardien de but de l'équipe nationale allemande de football, et de son épouse ont été publiées dans un magazine. Les journalistes ont été condamnés à une amende car ils avaient violé le droit à la vie privée de la famille. Toutes les photos montraient les enfants en compagnie de leurs parents ou en vacances, alors que le sujet des reportages n'était pas les enfants eux-mêmes, mais plutôt la relation de leurs parents et la carrière d'Oliver Kahn.
- Dans l'affaire Reklos et Davourlis c. Grèce, la prise de photos d'un nouveau-né sans le consentement de ses parents (dans l'unité de soins intensifs à laquelle seul le personnel de l'hôpital aurait dû avoir accès) a été considérée comme une violation du droit au respect de la vie privée, même si les photos n'ont pas été publiées".

Notez que cette dernière phrase est particulièrement pertinente, car elle met l'accent sur la nécessité de disposer d'une base juridique pour le traitement des données au moment où les photographies sont prises. La décision de ne pas les publier permet seulement d'éviter un traitement illicite ultérieur (publication), mais ne répare pas la violation antérieure du droit à la vie privée.

6.4 Points à retenir

Il existe quelques conseils qui peuvent servir de résumé des choses que vous devez savoir sur la conformité en matière de protection des données. En général, vous devez toujours garder à l'esprit ce qui suit :

- La publication de données à caractère personnel implique un traitement des données. Par conséquent, vous devez vous assurer que vous êtes autorisé à montrer ces données avant de procéder à leur publication. À ce moment-là, vous devez avoir une base juridique qui autorise le traitement. Dans le cas contraire, le traitement serait illégal.
- Si les données à caractère personnel sont traitées dans le but de servir l'intérêt public ("fins journalistiques"), il est probable que le traitement ne devra pas se conformer à certains ou à tous les articles du GDPR. À l'inverse, cela signifie que si les données personnelles sont collectées, analysées ou traitées pour d'autres raisons, le GDPR s'appliquera pleinement.

- La publication d'informations sensibles peut causer un préjudice considérable à la vie privée de la personne concernée. Vous devez vous assurer que les avantages pour l'intérêt public justifient une telle atteinte. À cette fin, vous devez mettre en balance les intérêts en jeu, en considérant les différents niveaux d'intrusion dans la vie privée de la personne concernée. Ce n'est que lorsque les considérations d'intérêt public l'emportent clairement sur la vie privée de la personne concernée que vous êtes autorisé à publier ces informations.

- L'intervention de la direction de la rédaction ou le recours à des experts peut être d'une grande aide pour garantir le respect de cette exigence. N'oubliez jamais que les journalistes intéressés ne sont généralement pas aussi objectifs lorsqu'ils mettent en balance les différents intérêts en jeu.

- N'oubliez jamais que vous ne devez recueillir que des données pertinentes pour votre enquête et susceptibles de présenter un intérêt public. Si, par exemple, vous enquêtez sur un homme politique sur la base d'une éventuelle pratique de corruption et que vous découvrez des informations sensibles sur son orientation sexuelle, vous ne devez pas les traiter, à condition qu'elles ne soient pas pertinentes pour la question en jeu. Il s'agit d'une exigence essentielle du principe de minimisation, un concept clé du GDPR.

- Dans les cas particulièrement litigieux, lorsqu'il n'est pas tout à fait clair si ou dans quelle mesure l'"exemption journalistique" s'applique au traitement des données, une piste d'audit devrait être conservée afin d'expliquer les considérations relatives à la protection des données et la consultation de l'autorité de contrôle principale devrait être demandée (Biriukova, p. 30).

- Des précautions particulières doivent être adoptées en cas de traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi qu'en cas de traitement de données génétiques, de données relatives à la santé ou de données relatives à la vie sexuelle ou aux condamnations et infractions pénales ou aux mesures de sécurité y afférentes.

- Les données concernant la population vulnérable et en particulier les mineurs ne doivent être traitées que si des raisons fortes le justifient. Vous devez être absolument sûr qu'elles s'appliquent au traitement concret avant de procéder.

7. Questions et réponses

Qu'en est-il de l'utilisation secondaire des données ?

La réponse à cette question dépend de quelques points essentiels. Tout d'abord, si les données ont été collectées sur la base d'un intérêt légitime, d'un contrat ou d'intérêts vitaux, elles peuvent être utilisées pour une autre finalité, pour autant que cette nouvelle finalité soit compatible avec la finalité initiale. Conformément à l'article 6.4 du GDPR, il convient de prendre en compte, entre autres, les éléments suivants :

a. tout lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
b. le contexte dans lequel les données personnelles ont été collectées, notamment en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
c. la nature des données à caractère personnel, en particulier si des catégories particulières de données à caractère personnel sont traitées, conformément à l'article 9, ou si des données à caractère personnel relatives aux condamnations pénales et aux infractions sont traitées, conformément à l'article 10 ;
d. les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
e. l'existence de mesures de protection appropriées, qui peuvent inclure le cryptage ou la pseudonymisation.

Si l'on souhaite utiliser les données à des fins de statistiques ou de recherche scientifique, il n'est pas nécessaire d'effectuer le test de compatibilité. Ces nouvelles utilisations sont compatibles avec la finalité initiale, conformément à l'article 5.2 (b) du GDPR.

Si l'on traite les données sur la base du consentement des personnes concernées ou à la suite d'une obligation légale, aucun autre traitement n'est possible au-delà de ce qui est

couvert par le consentement initial ou les dispositions de la loi. Un traitement ultérieur nécessiterait l'obtention d'un nouveau consentement ou d'une nouvelle base juridique.

J'aimerais obtenir une mise au point sur les sujets impliqués dans la commercialisation des données personnelles, une évaluation économique du montant de ce système de trafic mondial.

En principe, la commercialisation des données n'est possible que si aucune donnée personnelle n'est impliquée. Dans le cas où un jeu de données mélange les deux types de données, le GDPR est applicable. Ainsi, la commercialisation des données ne serait pas acceptable. Les données personnelles sont liées à des droits. Elles ne sont pas des marchandises et ne peuvent pas être achetées ou vendues. Voir la partie des Lignes directrices PANELFIT consacrée aux ensembles de données et notre Analyse critique pour plus de données.

Conservation/stockage des données, droit à l'oubli

En général, les données ne doivent pas être conservées plus longtemps que ce qui est strictement nécessaire aux fins pour lesquelles elles ont été collectées. Si le responsable du traitement estime qu'elles pourraient être utiles à l'avenir, il doit justifier cet assortiment. En tout état de cause, elles doivent être conservées d'une manière qui s'accorde avec les principes de minimisation et de limitation du stockage. Ainsi, elles doivent être anonymisées ou, au moins, pseudonymisées chaque fois que possible.

Le droit à l'oubli est régi par l'article 17 du GDPR. Si les conditions énoncées à l'article 17.1 GDPR sont remplies, le responsable du traitement " a l'obligation d'effacer les données à caractère personnel sans retard excessif ". Néanmoins, il ne s'agit pas d'un droit absolu. Les exemptions de l'article 17.3 GDPR identifient les cas dans lesquels cette obligation ne s'applique pas. L'une de ces conditions est que le droit "ne s'applique pas dans la mesure où le traitement est nécessaire (...) à l'exercice du droit à la liberté d'expression et d'information" (article 17.3 (a)). Comment équilibrer les deux droits et intérêts - droit à l'effacement et droit à la liberté d'expression et d'information ? Selon ce qu'a expliqué la CJUE dans son arrêt Google 2, l'article 17.3.a GDPR est "une expression du fait que le droit à la protection des données à caractère personnel n'est pas un droit absolu mais (...) doit être considéré en relation avec sa fonction dans la

société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité".[14] La Cour "énonce expressément l'exigence de trouver un équilibre entre les droits fondamentaux à la vie privée et à la protection des données à caractère personnel garantis par les articles 7 et 8 de la Charte, d'une part, et le droit fondamental à la liberté d'information garanti par l'article 11 de la Charte, d'autre part."[15] D'autre part, la CEDH a indiqué dans l'arrêt " M.L. et W.W. contre Allemagne " du 28 juin 2018, le que la mise en balance des intérêts pouvait difficilement se résoudre en faveur d'une demande d'effacement dirigée contre l'éditeur initial dont l'activité est au cœur de ce que la liberté d'expression vise à protéger.[16] Ainsi, de manière générale, le droit à l'oubli ne s'applique pas s'il entrave l'exercice du droit à l'information.

Collecte de données dans le cadre d'enquêtes, stockage de données, traitement de données provenant de sources confidentielles

Le secret professionnel est une valeur fondamentale qui ne devrait pas être brisée sur la base de la protection des données. Très probablement, votre État membre a adopté des règles spécifiques pour définir les pouvoirs des autorités de contrôle prévus à l'article 58, paragraphe 1, points e) et f), à l'égard des responsables du traitement ou des sous-traitants qui sont soumis, en vertu du droit de l'Union ou des États membres ou de règles établies par des organismes nationaux compétents, à une obligation de secret professionnel ou à d'autres obligations de secret équivalentes lorsque cela est nécessaire et proportionné pour concilier le droit à la protection des données à caractère personnel et l'obligation de secret (Voir l'article 90 du GDPR). Ces règles ne s'appliquent toutefois qu'aux données à caractère personnel que le responsable du traitement ou le sous-traitant a reçues à la suite d'une activité couverte par cette obligation de secret ou qu'il a obtenues dans le cadre de celle-ci.

Recherche/enquête médico-légale avec l'apprentissage automatique et les faux résultats de ces approches qui affectent les citoyens.

Les journalistes sont censés vérifier soigneusement l'exactitude de leurs informations. Les données déduites sont des données personnelles, car elles fournissent des

14 CJUE, affaire C-136/17, arrêt du 24 septembre 2019, point 57.

15 CJUE, affaire C-136/17, arrêt du 24 septembre 2019, point 59.

16 Cour européenne des droits de l'homme (CEDH), " M.L. et W.W. c. Allemagne ", 28 juin 2018.

informations sur une personne identifiable. Tous les droits et devoirs établis par le GDPR leur sont applicables.

Outils spécifiques qui pourraient rendre le traitement des données plus facile à gérer

Le manuel PANELFIT pour les journalistes et les lignes directrices pourraient être très utiles à ces fins.

Le cycle de vie du traitement des données. Si vous pouvez conserver des données ou, par exemple, des enregistrements d'entretiens, quand devez-vous les supprimer ? Les meilleures pratiques pour distinguer ce qui peut être conservé indéfiniment de ce qui doit être supprimé, et pour prendre le temps de supprimer réellement les éléments pertinents des emplacements de sauvegarde après un certain nombre d'années.

Il n'y a rien qui ressemble à une norme objective de durée de stockage adéquate dans le GDPR. Cela dépend totalement du fait que le stockage ait un sens ou non. Si vous pouvez prouver que le stockage de ces données est nécessaire à la finalité du traitement, vous pouvez les conserver indéfiniment. Dans tous les cas, elles doivent être stockées d'une manière qui fonctionne bien avec les principes de minimisation et de limitation du stockage. Ainsi, elles doivent être anonymisées ou, au moins, pseudonymisées chaque fois que possible.

Règlement relatif aux informations sur la santé

" Les données à caractère personnel qui sont, par nature, particulièrement sensibles au regard des droits et libertés fondamentaux méritent une protection spécifique car le contexte de leur traitement pourrait créer des risques importants pour les droits et libertés fondamentaux " (considérant 51 du GDPR). Les données concernant la santé sont considérées comme des catégories particulières de données à caractère personnel. Selon l'article 9.1, elles ne peuvent pas être traitées, à moins qu'il n'y ait une exception qui autorise un tel traitement. Les exceptions sont énumérées à l'article 9, paragraphe 2.

Protection des images

Les images sont des données à caractère personnel. Il faut donc une base légale pour traiter ces données. Si les images correspondent à plusieurs personnes, la base juridique doit s'appliquer à toutes les personnes concernées. Par exemple, si la base de données

est le consentement, vous devez avoir le consentement de toutes les personnes qui figurent sur la photographie ou la vidéo. Bien sûr, l'intérêt public peut être une excellente base juridique pour autoriser le traitement, mais vous devez soigneusement mettre en balance les droits, les libertés et l'intérêt en jeu. Par exemple, si vous pouvez éviter d'identifier les personnes qui ne sont pas essentielles à l'information, vous devriez le faire, surtout s'il s'agit de mineurs.

Comment traiter les données accessibles au public dans un format non structuré dans le but de compiler un nouvel ensemble de données qui pourrait éventuellement conduire à des informations précieuses, mais aussi nuire aux personnes vulnérables (par exemple, en récupérant des données personnelles [publiques] sur un média social) ?

En général, vous devez toujours trouver une base juridique appropriée pour le traitement des données. Comme indiqué précédemment, l'intérêt légitime est, en l'absence de consentement, la base la plus appropriée. Si nous parlons de la population vulnérable, celle-ci doit figurer en bonne place dans le test de mise en balance. Le traitement ne serait licite que si l'intérêt public est si fort qu'il l'emporte sur l'intérêt de la personne concernée.

Le scrapping en tant que tel n'introduit pas de nouveautés dans cette règle de base. Même si certaines données sont publiques, cela ne signifie pas que vous pouvez les utiliser comme vous le souhaitez. Dans le cas de données qui sont exprimées dans un réseau social, vous devez également tenir compte du fait que vous êtes également un utilisateur de ce réseau. Ainsi, les conditions d'utilisation vous sont applicables. En principe, cela ne devrait pas signifier grand-chose, mais vous devriez le garder à l'esprit.

Des informations détaillées à ce sujet sont disponibles ici :

Moreno Mancosu, Federico Vegetti, What You Can Scrape and *What Is Right to Scrape : A Proposal for a Tool to Collect Public Facebook Data, Social media + Society*, Volume : 6 issue : 3, Article first published online : 31 juillet 2020 ; Numéro publié : 1er juillet 2020, à l'adresse : https://journals.sagepub.com/doi/full/10.1177/2056305120940703

Comment se comporter lorsque vous souhaitez envoyer un communiqué de presse à l'adresse électronique professionnelle d'un autre journaliste (en supposant que vous n'ayez pas eu de contact préalable). Devez-vous demander l'autorisation au préalable (et comment, si ce n'est pas par courrier électronique) ou devez-vous présumer qu'il a un intérêt à être informé, donc lui envoyer votre communiqué de presse et lui donner la possibilité de refuser ? Et qu'en est-il des courriels de suivi ?

En général, vous pouvez envoyer des courriels aux adresses professionnelles des gens, à condition que :

- vous avez une bonne raison de penser que le destinataire peut bénéficier des informations fournies par le communiqué de presse.
- vous devez informer le destinataire des données à caractère personnel que vous traitez, de la finalité du traitement et de la manière dont il peut retirer ses données de votre liste de diffusion ou les modifier, au cas où cette liste existerait.
- En outre, vous ne devez pas traiter les données personnelles des destinataires (stockage, par exemple) plus longtemps que nécessaire.

L'envoi de suivis ne viole pas le GDPR s'il répond aux trois exigences décrites dans la réponse ci-dessus. Le traitement des données dans le cas d'un message de suivi doit suivre les mêmes règles qu'un message préliminaire.

8. Glossaire (art. 4 GDPR)

1) «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

2) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utili- sation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rappro- chement ou l'interconnexion, la limitation, l'effacement ou la destruction;

3) «limitation du traitement», le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur;

4) «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

5) «pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisa- tionnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

6) «fichier», tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

7) «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

8) «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

9) «destinataire», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

10) «tiers», une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

11) «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

12) «violation de données à caractère personnel», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

13) «données génétiques», les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la

physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question;

14) «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques;

15) «données concernant la santé», les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne;

16) «établissement principal»,

a) en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son adminis- tration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;

b) en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement;

17) «représentant», une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du présent règlement;

18) «entreprise», une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique;

19) «groupe d'entreprises», une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle;

20) «règles d'entreprise contraignantes», les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe;

21) «autorité de contrôle», une autorité publique indépendante qui est instituée par un État membre en

vertu de l'article 51;

22) «autorité de contrôle concernée», une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que:

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

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

c) une réclamation a été introduite auprès de cette autorité de contrôle;

23) «traitement transfrontalier»,

a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou

b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établis- sement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres;

24) «objection pertinente et motivée», une objection à un projet de décision quant à savoir s'il y a ou non violation du présent règlement ou si l'action envisagée en ce qui concerne le responsable du traitement ou le sous-traitant respecte le présent règlement, qui démontre clairement l'importance des risques que présente le projet de décision pour les libertés et droits fondamentaux des personnes concernées et, le cas échéant, le libre flux des données à caractère personnel au sein de l'Union;

25) «service de la société de l'information», un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535 du Parlement européen et du Conseil ([1]);

26) «organisation internationale», une organisation internationale et les organismes de droit public international qui en relèvent, ou tout autre organisme qui est créé par un accord entre deux pays ou plus, ou en vertu d'un tel accord.

Annexe I. Le test de mise en balance

Introduction : Le test de mise en balance dans le contexte de l'intérêt légitime comme base juridique du traitement

L'intérêt légitime est l'une des six bases légales pour le traitement des données à caractère personnel énoncées à l'article 6, paragraphe 1, du GDPR. Cette base juridique exige que les intérêts légitimes du responsable du traitement ou de tout tiers auquel les données sont communiquées prévalent sur les intérêts, les droits fondamentaux et les libertés des personnes concernées (article 6, paragraphe 1, point f). Pour vérifier que c'est bien le cas, les responsables du traitement peuvent recourir à un outil appelé "balancing test", qui a été recommandé par le groupe de travail "Article 29", par exemple[17]. Cet outil vise à garantir que les intérêts légitimes du responsable du traitement ou de tout tiers auquel les données sont communiquées prévalent sur les intérêts et les libertés et droits fondamentaux des personnes concernées.

Quand les droits et libertés fondamentaux de la personne concernée par la protection des données ne priment-ils pas ?

La réalisation d'un test de mise en balance implique la prise en compte de plusieurs facteurs clés qui sont décisifs pour déterminer quels intérêts, libertés ou droits prévalent, à savoir [18]:

- la **nature et la source de l'intérêt légitime** - si le traitement des données est nécessaire à l'exercice d'un droit fondamental, s'il est par ailleurs d'intérêt public ou s'il bénéficie d'une reconnaissance dans la communauté concernée. L'évaluation du préjudice éventuel subi par le responsable du traitement, par des tiers ou par la collectivité en général si le traitement des données n'a pas lieu est obligatoire.
- Le **pouvoir et le statut des deux parties** (responsable du traitement ou tiers et personne concernée). Par exemple, un employeur qui a l'intention de traiter les

17 A29WP, Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement au titre de l'article 7 de la directive 95/46/CE. Avril 2014, p.24. À l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consulté le 05 janvier 2020

18 A29WP, Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement au titre de l'article 7 de la directive 95/46/CE. Avril 2014, p.24. À l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consulté le 05 janvier 2020.

données d'un employé est dans une position plus forte que l'employé. Si la personne concernée est un mineur, ses intérêts, droits ou libertés doivent être pris en compte.

- La **nature des données**. Les données relatives à des catégories spéciales, par exemple, doivent être davantage prises en compte. De même, les données que les gens sont susceptibles de considérer comme particulièrement "privées" (par exemple les données financières), les données relatives aux enfants ou à d'autres personnes vulnérables doivent être pondérées de manière adéquate.

- L'**impact du traitement sur les personnes concernées**. À cette fin, les responsables du traitement doivent examiner si le traitement peut entraîner un risque élevé pour les droits et libertés des personnes. Si tel est le cas, ils doivent effectuer une évaluation des risques liés au traitement.
- **Les attentes raisonnables** des personnes concernées quant à ce qu'il adviendra de leurs données. Les responsables du traitement doivent être en mesure de démontrer qu'une personne raisonnable s'attendrait au traitement à la lumière des circonstances particulières applicables. Si la finalité et la méthode de traitement ne sont pas immédiatement évidentes et qu'il existe un potentiel d'opinions raisonnables sur la question de savoir si les personnes s'y attendraient, les responsables du traitement peuvent souhaiter mener une forme de consultation, de groupe de discussion ou d'étude de marché avec les personnes afin de démontrer les attentes et de soutenir leur position. S'il existe des études préexistantes sur les attentes raisonnables dans un contexte particulier, les responsables du traitement peuvent s'en inspirer pour déterminer ce que les personnes peuvent attendre ou non[19].

- La **manière dont les données sont traitées** (grande échelle, exploration de données, profilage, divulgation à un grand nombre de personnes ou publication);

- Les **garanties supplémentaires** qui pourraient limiter l'impact indu sur la personne concernée, telles que la minimisation des données (par ex. des limitations strictes de la collecte des données ou la suppression immédiate des données après leur utilisation) - des mesures techniques et organisationnelles visant à garantir que les données ne peuvent pas être utilisées pour prendre des décisions ou d'autres mesures concernant les personnes ("séparation fonctionnelle") - une large utilisation des techniques d'anonymisation, l'agrégation des données, les technologies renforçant la protection de la vie privée, le respect de la vie privée dès la conception, les évaluations d'impact sur la vie privée et la protection des données ; une transparence accrue, un droit d'opposition général et inconditionnel (opt-out), la portabilité des données et des mesures connexes visant à responsabiliser les personnes concernées, etc.

La question de la sauvegarde supplémentaire

19 ICO, Comment appliquons-nous les intérêts légitimes dans la pratique ? À l'adresse : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Consulté : 15 janvier 2020

Le groupe de travail "Article 29" estime que les mesures d'atténuation et les garanties, telles que les mesures organisationnelles ou techniques adoptées par le responsable du traitement pour la protection des droits de la personne concernée, devraient être incluses dans le test de mise en balance. Il existe toutefois une autre approche, qui considère que l'article 6, paragraphe 1, point f), demande une mise en balance entre deux valeurs, les intérêts légitimes du responsable du traitement (ou d'un tiers) et les intérêts, droits et libertés de la personne concernée. Les mesures d'atténuation et les garanties ne correspondent à aucune de ces valeurs. Par conséquent, ils ne doivent pas être envisagés. Dans le cas contraire, ils l'emporteraient sur le point de vue des responsables du traitement, car ils réduiraient l'importance du préjudice éventuel causé aux intérêts, aux droits et aux libertés de la personne concernée. Kamara et De Hert ont fait des déclarations convaincantes sur cette question concrète, en affirmant que[20]

> *"L'inclusion de mesures d'atténuation dans l'évaluation conduirait à une représentation de l'impact réel attendu du traitement sur les droits des personnes concernées, et permettrait toujours aux intérêts légitimes de prévaloir. Cette approche ne "punit" pas le responsable du traitement qui prend des mesures d'atténuation et des garanties, en ne les incluant pas dans le test de mise en balance. Au contraire, elle encourage le responsable du traitement à le faire. Par ailleurs, il convient de garder à l'esprit que le poids des mesures de sauvegarde et d'atténuation futures est toujours fonction de leur mise en œuvre et de leur efficacité. Ces mesures doivent donc être prises en considération, mais ne doivent pas jouer un rôle important pour déterminer de quel côté penche la balance."*

Quelques exemples de tests d'équilibre

Exemple 1[21]

Cas : Le journal Z envisage de publier des photographies montrant X, un acteur, après avoir été arrêté pour possession de cocaïne lors d'une parade publique. X est un personnage public célèbre dans son pays car il joue un policier dans une série télévisée.

20 Kamara, Irène et De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground : a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. À l'adresse : https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Consulté le : 17 janvier 2020

21 Source : A29WP, Avis 06/2014 sur la notion d'intérêts légitimes du responsable du traitement au titre de l'article 7 de la directive 95/46/CE. Avril 2014, p.63. À l'adresse : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Consulté le 05 janvier 2020

En outre, il a concédé plusieurs interviews fournissant publiquement des données sur sa vie privée.

Test d'équilibre : les données concernent la vie privée de l'individu plutôt que sa vie professionnelle. Le partage de ces données pourrait causer un préjudice important à la personne concernée. Cependant, il existe un intérêt public à partager ces informations. L'espoir de l'acteur que sa vie privée sera effectivement protégée a été réduit par le fait qu'il a divulgué des données de sa vie privée dans plusieurs interviews. Après avoir examiné tous les facteurs pertinents, l'entreprise doit conclure que les intérêts de l'acteur célèbre ne l'emportent pas sur ses intérêts légitimes à publier les photographies, et que le traitement est licite sur la base de ces intérêts légitimes.

Voir : Axel Springer AG contre Alemania

Exemple 2[22]

Cas : Un employeur surveille l'utilisation d'Internet par ses employés pendant les heures de travail pour vérifier qu'ils ne font pas un usage personnel excessif de l'informatique de l'entreprise. Les données collectées comprennent les fichiers temporaires et les cookies générés sur les ordinateurs des employés, indiquant les sites web visités et les téléchargements effectués pendant les heures de travail. Les données sont traitées sans consultation préalable des personnes concernées et des représentants syndicaux/du comité d'entreprise de l'entreprise. En outre, les personnes concernées ne sont pas suffisamment informées de ces pratiques.

Test d'équilibre : La quantité et la nature des données collectées constituent une intrusion importante dans la vie privée des employés. Outre les questions de proportionnalité, la transparence des pratiques, étroitement liée aux attentes raisonnables des personnes concernées, est également un facteur important à prendre en considération. Même si l'employeur a un intérêt légitime à limiter le temps passé par les employés à visiter des sites web sans rapport direct avec leur travail, les méthodes utilisées ne répondent pas au critère de mise en balance de l'article 7, point f). L'employeur devrait utiliser des méthodes moins intrusives (par exemple, limiter

22 Source : ICO. Comment appliquer les intérêts légitimes dans la pratique ? À l'adresse : https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Consulté : 15 janvier 2020

l'accessibilité de certains sites), qui sont, en tant que meilleure pratique, discutées et convenues avec les représentants des employés, et communiquées aux employés de manière transparente.

À faire et à ne pas faire

Dos

- Vérifiez la nature des données traitées et veillez à protéger les intérêts, les droits et les libertés des enfants s'ils sont en jeu.
- Tenir compte des attentes raisonnables des personnes concernées
- Effectuer un DPIA si les circonstances le recommandent

À ne pas faire

- Ne traitez pas les données des enfants si cela n'est pas absolument nécessaire pour atteindre l'intérêt poursuivi
- Ne traitez pas les données si le test d'équilibrage n'est pas concluant.
- N'hésitez pas à mettre en place des garanties adéquates pour minimiser les atteintes aux intérêts, droits et libertés des personnes concernées.

Liste de contrôle

- Les responsables du traitement se sont assurés que les intérêts de la personne ne prévalent pas sur les intérêts légitimes du responsable du traitement ou de tiers.
- Les responsables du traitement utilisent les données des individus de la manière à laquelle ils peuvent raisonnablement s'attendre.
- Les responsables du traitement n'utilisent pas les données des personnes de manière très intrusive ou d'une manière qui pourrait leur porter préjudice, sauf s'ils ont une raison particulièrement valable.
- Les responsables du traitement ne traitent pas les données des enfants ou, s'ils le font, ils ont pris des précautions supplémentaires pour s'assurer qu'ils protègent leurs intérêts.
- Les contrôleurs ont envisagé des mesures de sauvegarde pour réduire l'impact dans la mesure du possible.
- Les contrôleurs ont examiné s'ils devaient mener une DPIA.

Autres lectures

- Des exemples supplémentaires de tests d'équilibrage ont été fournis par l'Article 29WP et peuvent être trouvés dans leur avis 06/2014 sur la notion d'intérêts légitimes du contrôleur en vertu de l'article 7 de la directive 95/46/CE.

- A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

- EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 april 2017, at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Accessed 5 May 2020

- ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

- ICO, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Accessed 05 May 2020.

- Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Annexe II. Analyse comparative du cadre réglementaire au niveau des États membres de l'UE

La source principale des informations recueillies est l'analyse comparative Bird&Bird, sauf indication contraire.

Autriche

Dernière révision : 05.06.2018

La section 9 de l'ADPA prévoit des dispositions spéciales concernant le traitement des données à caractère personnel dans le cadre de la liberté d'expression et d'information. Selon ces dispositions, plusieurs règlements du GDPR (notamment ses principes et les droits des personnes concernées) ne s'appliquent pas au traitement des données personnelles à des fins journalistiques ainsi qu'à des fins scientifiques, artistiques ou littéraires.

Belgique

Dernière révision : 13.09.2018

L'article 16 de la LPD autorise le traitement des données à caractère personnel effectué par des moyens adéquats à des fins journalistiques ou à des fins d'expression académique, artistique ou littéraire. Les articles 17 et suivants stipulent les exceptions aux obligations d'information (article 17), la protection de la source et du contenu des informations (article 18), les exceptions au droit à la restriction du traitement (article 19), l'information sur la rectification et l'effacement (article 20) et la limitation du droit d'opposition (article 21).

Finlande

Dernière révision : 13.11.2018

Selon l'article 27 de la loi sur la protection des données, seules des dispositions limitées du GDPR s'appliquent au traitement des données personnelles à des fins de journalisme ou d'expression académique, artistique ou littéraire. Cette approche maintient la situation telle qu'elle était sous la loi abrogée sur les données personnelles.

France

Dernière révision : 11.02.2019

Selon le cadre réglementaire français, lorsque des données à caractère personnel sont traitées à des fins d'expression journalistique, artistique ou littéraire, les dispositions

relatives à la notification d'informations, aux transferts de données, aux données sur les droits des personnes concernées, à la conservation et au traitement de catégories particulières de données ne s'appliquent pas.

Allemagne

Dernière révision : 23.05.2018

§ L'article 35 de la nouvelle loi fédérale allemande sur la protection des données ("FDPA") dispense le responsable du traitement de l'obligation d'effacer les données à caractère personnel lorsque l'effacement est, en cas de traitement non automatique des données, impossible ou n'est possible qu'au prix d'efforts disproportionnés et que la personne concernée a un intérêt mineur à l'effacement. § L'article 27, paragraphe 2, de la loi sur la protection des données limite les droits des personnes concernées sous réserve de certaines exigences supplémentaires.

Irlande

Dernière révision : 07.06.2018

En vertu de l'article 43(1) de la loi, le traitement de données à caractère personnel aux fins de l'exercice du droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques ou à des fins d'expression académique, artistique ou littéraire, est exempté du respect de certaines dispositions du GDPR lorsque, compte tenu de l'importance du droit à la liberté d'expression et d'information dans une société démocratique, le respect de ces dispositions serait incompatible avec ces objectifs. La Commission de protection des données peut renvoyer toute question de droit impliquant l'examen de la question de savoir si le traitement des données à caractère personnel est exempté en vertu de l'article 43(1) à la Haute Cour pour qu'elle tranche.

Italie.

Dernière révision : 25.10.2018

IDPA titre XII - sections 136-137-138-139. Le code de pratique sur le traitement des données personnelles et les activités journalistiques (annexe A.1 de l'IDPA) reste en

vigueur. La compatibilité de ce code avec le GDPR sera réévaluée par l'Autorité italienne de protection des données (ci-après, l'"Autorité"). L'Autorité devrait l'examiner avant la fin du calendrier. En outre, l'Italie a intégré certains principes relatifs à l'exemption journalistique par le biais d'un code d'éthique, à savoir

a) l'obligation d'éviter toute forme de censure préalable

b) l'exemption du droit à l'information dans la collecte des données lorsque l'exercice professionnel l'exige

c) le devoir du journaliste de rectifier sans délai les erreurs et les inexactitudes

d) la nécessité d'être particulièrement prudent lorsque le traitement concerne des données spécialement protégées. Dans ces circonstances, le traitement est limité aux faits présentant un intérêt public incontestable. En outre, il doit se limiter aux aspects essentiels de l'information et éviter les références à des personnes sans lien avec elles. Même dans le cas de faits que l'intéressé a pu rendre publics, ou qui sont appréciés dans le comportement public, le droit à la protection est réservé

e) il est suggéré de rechercher l'"essentialité" de l'information, la proportionnalité de ce qui est rendu public, de sorte qu'il soit limité à ce qui est essentiel par rapport à l'affaire.

f) lorsqu'il s'agit d'une information relative à la santé, il convient de respecter la dignité, la bienséance et la vie privée de la personne concernée, notamment lorsqu'il s'agit de maladies graves ou terminales, en s'abstenant de publier des données analytiques ou d'intérêt strictement clinique. Toutefois, il peut être fait exception à cette exigence lorsque, conformément au principe de proportionnalité, la personne concernée se trouve dans une situation d'importance publique particulière. Il en va de même pour les informations sur la vie sexuelle.

Les Pays-Bas

Dernière révision : 17.09.2018

L'article 41 de l'acte d'exécution du GDPR prévoit que l'ordre d'exécution du GDPR ne s'applique pas lorsque les données personnelles sont traitées exclusivement à des fins journalistiques ou à des fins d'expressions académiques, artistiques ou littéraires. En

outre, il résume une liste de chapitres et d'articles du GDPR qui ne sont pas non plus applicables à ces fins : (a) l'article 7, paragraphe 3, l'article 11, paragraphe 2 ; b) le chapitre III ; c) le chapitre IV (à l'exception des articles 24, 25, 28, 29 et 32) ; d) le chapitre V ; e) le chapitre VI ; et f) le chapitre VII. " L'art. 41 LAUV limite la portée de certaines obligations en lien avec des intérêts généraux (impérieux), en alignement avec l'art 23 GDPR. Il prévoit donc des exceptions aux droits de la personne concernée et aux obligations du responsable du traitement. Le GDPR partiellement (art. 12-21 et 34 GDPR) ne s'applique pas (dans la mesure où cela est approprié et proportionné) au traitement des données en vue - entre autres - d'objectifs d'intérêt public importants, de la sécurité publique, de la protection de la personne concernée ou des droits et libertés d'autrui ; et/ou du recouvrement des créances civiles.

Espagne

Dernière révision : 05.03.2019

La SDPA n'inclut aucun précepte juridique qui concilie la liberté d'expression et la protection des données. Il n'y a qu'une référence à la liberté d'expression dans l'article 85 concernant le droit à la liberté d'expression sur Internet que chacun possède.

Suède

Dernière révision : 06.09.2018

Loi sur la protection des données, paragraphe 1:7 : le GDPR et la loi sur la protection des données ne doivent pas être appliqués dans la mesure où cela violerait les lois sur la liberté d'expression. La loi sur la protection des données prévoit que les articles 5-30 et 35-50 du GDPR ne sont pas applicables au traitement des données personnelles à des fins journalistiques ou à des fins d'expressions académiques, artistiques ou littéraires.

Royaume-Uni

Dernière révision : 23.05.2018

La loi britannique de 2018[23] sur la protection des données offre une vision plus nuancée des limites de l'exemption, suggérant que certaines des dispositions du GDPR ne s'appliqueraient pas au traitement des données lorsque trois conditions cumulatives sont remplies (Cain, 2018) :

- les données en question doivent être traitées en vue de la publication de matériel journalistique,
- le responsable du traitement doit raisonnablement penser que, compte tenu notamment de l'importance particulière de l'intérêt public pour la liberté d'expression, la publication serait dans l'intérêt public, et
- le responsable du traitement des données doit raisonnablement penser que l'application de la disposition du GDPR citée serait incompatible avec sa finalité journalistique.

L'ICO britannique conseille d'examiner la deuxième condition - "l'intérêt public" - au cas par cas en tenant compte des codes de conduite existants et en mettant en balance l'intérêt public du sujet et le niveau d'intrusion dans la vie privée d'un individu. Il n'est pas surprenant de voir que l'"intérêt public" est l'un des critères retenus, car il figure en bonne place dans la jurisprudence de la Cour européenne des droits de l'homme. Bien que la Cour européenne des droits de l'homme se soit abstenue de donner une définition de l'"intérêt public", elle a reconnu que cette notion couvrait le débat public, politique et historique, les questions liées aux politiciens, le comportement des fonctionnaires, les grandes entreprises, les gouvernements, les questions liées à la criminalité. Toutefois, d'autres questions moins apparentes peuvent également être considérées comme répondant à l'intérêt public ou général (Bitiukowa, 21).

23 Vid. La loi britannique sur la protection des données de 2018, annexe 2, partie 5, par. 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

Les informations relatives aux exemptions et dérogations en bref

Le tableau suivant (Bitiukowa, 25) comprend une comparaison actualisée entre plusieurs États membres de l'UE concernant la réglementation des exceptions.

TABLE 3

The scope of the "Journalistic exemption" under the national law of the selected Member States

GDPR Article	Explanation of the Article	Sweden	United Kingdom	Lithuania	Romania
Article 5(1)(f)	Principle of integrity and confidentiality, which means that a data controller (e.g., a media undertaking) must put in place technical and organizational measures to ensure that the personal data it processes is protection from unauthorized disclosure, accidental loss, damage,etc.	Partially exempted[94] ***	Not exempted**	Not exempted	Exempted
Article 6	Lawfulness of processing, which means that each processing operation can only be considered lawful if a data controller can identify a lawful basis for it (consent, contract, public interest, etc.).	Exempted*	Exempted	Not exempted	Exempted
Articles 12-23	Rights of data subjects, meaning that the data controller should provide individuals with information about processing and respond to their requests.	Exempted	Partially exempted[95]	Exempted	Exempted
Article 28	Processor, which means that where a media undertaking outsources data processing to another entity (e.g., a data centre or a data analytics company), they must have a data processing agreement in place with it.	Exempted	Not exempted	Not exempted	Exempted

* **Not exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply with the rule** the content of which is explained in the second column.

** **Exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **does not have to comply with the rule** the content of which is explained in the second column.

*** **Partially exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply only with the certain aspects of the rule** the content of which is explained in the second column and in the relevant footnote.

Sources d'information

Bibliographie

Article 29 Working Party, RECOMMENDATION 1/97 Data protection law and the media. Adopted by the Working Party on 25 February 1997, at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. Last visited: 17/10/2020.

BIRD & BIRD, Personal data and freedom of expression, At: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression. Last visited: 17/10/2020.

BENEZIC, Dollores, Romania May Be Using GDPR to Intimidate Journalists, Liberties, 2018, At: https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384. Last visited: 17/10/2020.

BITIUKOVA, Natalija, Journalistic exemption under the european data protection law, Vilnius Institute for Policy Analysis, 2020, at: https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf. Last visited: 17/10/2020.

CAIN N. and COWPER-COLES, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.lexology.com/library/detail.aspx?g=b26433e1-0548-4a9d-8351-f720e737f811. Last visited: 17/10/2020.

CULLAGH K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf. Last visited: 17/10/2020.

DETREKŐI, Zsuzsa, GDPR in Hungary: A Road to Hell?, At: https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281. Last visited: 17/10/2020.

DRECHSLER L., The GDPR and Journalism. Protecting Privacy or a Break on Democratic Accountability?, 18 September 2018, https://brusselsprivacyhub.eu/publications/ws21.html. Last visited: 17/10/2020.

ECtHR, Guide on Article 8 of the European Convention on Human Rights, August 2020, at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last visited: 17/10/2020.

EDRI, Proceed with caution, at: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf. Last visited: 17/10/2020.

NIELSEN, Nikolaj. EU Warns Romania Not to Abuse GDPR Against Press, EU Observer (Nov. 12, 2018

REVENTLOW, Nani Jansen, Symposium on the GDPR and international law. Can the GDPR and freedom of expression coexist? At: https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist. Last visited: 17/10/2020.

The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf. Last visited: 17/10/2020.

WARNER, Bernhard, Online-Privacy Laws Come With a Downside, The Atlantic, 2019, at: https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/. Last visited: 17/10/2020.

Documents du Conseil de l'Europe

Convention for the protection of individuals with regard to the processing of personal data

Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership

Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors

Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

Declaration by the Committee of Ministers on the protection and promotion of investigative journalism (26 September 2007)

Resolution 2066 (2015), Media responsibility and ethics in a changing media environment, Parliamentary Assembly

Resolution 1843 (2011), The protection of privacy and personal data on the Internet and online media, Parliamentary Assembly

Resolution 1165 (1998), Right to privacy, Parliamentary Assembly

Resolution 1003 (1993), Ethics of Journalism, Parliamentary Assembly

Jurisprudence de la Cour Européenne des Droits de l'Homme

- A v. Norway, No. 28070/06, 9 April 2009
- Ageyev v. Russia, No. 7075/10, 18 April 2013
- Alkaya v. Turkey, No. 42811/06, 9 October 2012
- Armonienė v. Lithuania, No. 36919/02, 25 November 2008
- Axel Springer Ag v. Germany [GC], No. 39954/08, 7 February 2012
- Bédat v. Switzerland [GC], No. 56925/08, 29 March 2016
- Biriuk v. Lithuania, No. 23373/03, 25 November 2008 Björk Eiðsdóttir v. Iceland, No. 46443/09, 10 July 2012
- Bladet Tromsø and Stensaas v. Norway, No. 21980/93, 20 May 1999

- Bodrožić v. Serbia, No. 32550/05, 23 June 2009 Bohlen v. Germany No. 53495/09 and Ernst August von Hannover v. Germany No. 53649/09, 19 February 2015
- Couderc and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
- Dorothea Sihler-Jauch against Germany and Günther Jauch v. Germany, Nos. 68273/10 and 34194/11, 24 May 2016 (decision)
- Egeland and Hanseid v. Norway, No. 34438/04, 15 April 2009
- Erla Hlynsdóttir (No.2), No. 54125/10, 21 October 2014
- Feldek v. Slovakia, No. 29032/95, 12 July 2001 Flinkkilä and Others v. Finland, No. 25576/04, 6 April 2010
- Fürst-Pfeifer v. Austria, Nos. 33677/10 and 52340/10, 17 May 2016
- Guseva v. Bulgaria, No. 6987/07, 17 February 2015
- Hachette Filipacchi Associés v. France, No. 71111/01, 14 June 2007
- Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
- Hachette Filipacchi Associés ("Ici Paris") v. France, No. 12268/03, 23 July 2009
- Haldimann and Others v. Switzerland, No. 21830/09, 24 February 2015
- Janowski v. Poland, No. 25716/94, 21 January 1999
- Khan v. Germany, No. 38030/12, 21 September 2016
- Khmel v. Russia, No. 20383/04, 12 December 2012
- Khuzhin and Others v. Russia, No. 13470/02, 23 October 2008
- Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 February 2002
- Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria, No. 33497/07, 17 January 2012
- Leempoel & S.A. ED. Ciné Revue v. Belgium, No. 64772/01, 9 November 2006
- Lillo-Stenberg and Sæther v. Norway, No. 13258/09, 16 January 2014 Mitkus v. Latvia, No. 7259/03, 2 October 2012
- MGN Limited v. the United Kingdom, No. 39401/04, 18 January 2011
- Mosley v. the United Kingdom, No. 48009/08, 10 May 2011
- Müller v. Germany (Dec.), No. 43829/07, 14 September 2010
- Österreichischer Rundfunk v. Austria, No. 35841/02, 7 December 2006 Guidelines on Safeguarding Privacy in the Media 38

- Peck. V. United Kingdom, No. 44647/98, 28 January 2003 Pentikäinen v. Finland [GC], No. 11882/10, 20 October 2015 Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009 Renaud v. France, No. 13290/07, 25 February 2010
- Salihu and Others v. Sweden, No. 33628/15, 10 May 2016 (decision)
- Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland, No. 34124/06, 21 June 2012
- Selistö v. Finland, No. 56767/00, 16 November 2004
- Standard Verlags GmbH v. Austria (No.2), No. 21277/05, 4 June 2009
- Standard Verlags GmbH v. Austria (No. 3), No. 34702/07, 10 January 2012
- Toma v. Romania, No. 42716/02, 24 February 2009
- Verlagsgruppe News GmbH v. Austria, No. 10520/02, 14 December 2006
- Von Hannover v. Germany, No. 59320/00, 24 June 2004
- Von Hannover v. Germany (No.2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012
- White v. Sweden, No. 42435/02, 19 September 2006
- Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no.2), No. 62746/00, 14 November 2002 (decision)
- Y v. Switzerland, No. 22998/13, 06 June 2017
- Zvagulis v. Lithuania, No. 8619/09, 26 January 2017 (decision)