Numérique et droit

Poullet, Yves

Published in:
Vie privée, liberté d'expression et démocratie dans la société numérique

Publication date:
2020

Document Version
le PDF de l'éditeur

Numérique et droit – La vertu du clair-obscur[1]

Yves Poullet

Professeur émérite à l'Université de Namur

Professeur associé à l'UCLille

Résumé

La transparence est devenue une valeur en soi tant elle apparaît inhérente à notre volonté de démocratie. On ajoute que la numérisation de la société lui donne dorénavant les moyens de son effectivité. Dans le monde de l'Internet, la transparence universelle y compris de sa vie est à portée d'un clic le secret est devenu suspect à tel point que l'exhibitionnisme a remplacé la pudeur et que se proclame la vérité selon laquelle seul celui qui a quelque chose à cacher se réclame du secret. Même les secrets professionnels et des communications s'évaporent dans nos réseaux complexes et face à la revendication sociétaire de sécurité. Reste à s'interroger sur la valeur de ce dogme du 'droit à la transparence'.

À y regarder de près. La réponse est complexe. Une transparence pour quoi faire et pour qui ? Un secret : pour quoi faire et pour qui ?

Le droit à la transparence est d'abord celui des citoyens vis-à-vis des administrations, plus récemment de ses dirigeants voire des lobbyings. Si la transparence est au service d'un État démocratique soucieux de

[1] Une première version de cet article avait été rédigée dans le cadre du Colloque « Conflits à l'ère numérique – la fin de l'utopie Internet » – Bruxelles Laïque – 18/10/2017 – Fondation Henri La Fontaine. Les Actes de ce colloque ont été publiés dans l'ouvrage collectif, *La fin de l'utopie Internet ? Les enjeux de la société numérique*, Éditions du Centre d'Action laïque, juin 2017, pp. 33 à 100. Ce texte est à jour au 1er juin 2019. Il a servi de base à la définition du programme du colloque. certains points développés par le texte sont repris par d'autres contributions, en particulier celles de Th. Leonard et A. Lachapelle.

la liberté des citoyens, cet objectif implique qu'elle soit proportionnée à cette finalité et que le secret réclamé tant par l'intérêt général (voir l'affaire *Wikileaks*) que par l'intérêt privé à la confidentialité soit respecté dans un monde où les TIC accroissent les risques de divulgation. Enfin, on note que la transparence qui justifiait une attitude purement passive de nos administrations, exige d'elles, dorénavant avec les vertus de l'électronique, une attitude proactive au service des entreprises et des citoyens.

Dans le secteur privé, l'affirmation du dogme de la transparence ne peut signifier la transparence unilatérale d'un acteur vis-à-vis de l'autre, celui des consommateurs qui permettra à l'entreprise de profiler, prédire et conduire l'action de ceux-ci. Le numérique réclame une transparence réciproque, une symétrie d'informations entre l'entreprise et les personnes concernées envisagées non individuellement mais associées. Au-delà il nous paraît indispensable dans une société de l'information ubiquitaire, de protéger les droits relatifs à l'anonymat et à la « séclusion », indispensables à assurer le développement de la spécificité de chaque individu, nécessaire dans une société démocratique.

Le débat entre secret et transparence se joue également en ce qui concerne l'accès aux savoirs. La « propriété » intellectuelle de l'information constitue souvent un outil permettant de mettre à profit l'exclusivité de l'information. Rarement – c'est le cas dans les mouvements *d'open source, open data* et *open document* – l'accès au savoir prime l'intérêt de l'auteur voire du soi-disant auteur. Le droit se met ainsi au service du secret.

La transparence des ordinateurs et des communications au profit des autorités policières et services secrets est réclamée au nom de la sécurité. La vie privée et les secrets professionnels s'évanouissent lorsqu'il s'agit de lutter contre ce qui met en cause la vie en société. Certes, mais les définitions larges des causes de justification, la globalisation et les possibilités technologiques de pénétrer les secrets des ordinateurs créent le risque d'un déséquilibre au profit d'une société de surveillance et de « conformisme anticipatif », ce qui est le contraire de l'idéal démocratique.

Enfin que dire des législations qui, au nom de l'égalité de tous devant l'impôt ou afin d'éviter fraudes fiscale ou sociale, encouragent la dénonciation y compris publique et ce sans respect des droits de la défense. Est-ce ainsi qu'il faut comprendre la citoyenneté ?

En conclusion, nous nous interrogerons sur le besoin d'une réflexion publique sur l'éthique du secret et de la transparence à l'heure des technologies du numérique. Il s'agit de déterminer les points d'équilibre entre ces deux valeurs en conflit, valeurs qui ne peuvent être posées en absolu mais doivent l'une et l'autre se juger en fonction de leur apport à la démocratie et aux libertés.

Introduction

« La transparence paraît se confondre avec la limpidité, la pureté même. Elle ressemble au soleil et à la lumière. Elle ne peut souffrir des domaines interdits, le mensonge, le mystère, le secret, la discrétion, tous les artifices qui dissimulent la vérité. Au nom de la transparence, le droit de l'information tend à devenir un droit absolu. Les images qui restent dans l'ombre, les paroles qui se disent sous le sceau de la confidence, deviennent suspectes »[2].

1. La citation du célèbre avocat et romancier français reprise en exergue de notre contribution apparaît, 18 ans après avoir été écrite, prémonitoire. Le dogme de la transparence et, corrélativement, la suspicion vis-à-vis du secret s'imposent chaque jour un peu plus dans nos sociétés de l'information. Comme l'écrivait Sauvé[3], « la première conséquence du développement de ces technologies est un renversement quasi complet de perspective. Alors que, dans la tradition, c'est-à-dire le monde matériel, le secret ou, à tout le moins, l'intimité sont la règle et la publicité, la dérogation ou l'exception qui exige une action consciente ou délibérée, à l'inverse la transparence est […] inhérente à la révolution numérique. Les technologies de l'information induisent une seconde évolution : elles modifient en effet le sens même de la notion de transparence et favorisent une revendication croissante de transparence totale de la vie publique et des individus ». L'assertion du droit absolu à l'information mérite cependant certaines nuances pour le juriste. Aux yeux du droit, en effet, tout ne doit pas être transparent, comme en témoigne la consécration récente de la protection des secrets d'affaires et il semble que le droit, tantôt, hésite avant d'emboîter le pas aux tenants du dogme de la transparence ; tantôt, reconnaît la légitimité de sa réclamation et donne à cette transparence les moyens de triompher. Notre propos entend étudier ces hésitations du droit, partagé entre, d'une part, la revendication démocratique à la clarté de notre environnement et de nos actions et, d'autre part, la défense d'une zone d'obscurité sans laquelle les individus et de manière plus large les relations interpersonnelles ne peuvent survivre et se développer.

[2] J.D. Bredin, « Secret, transparence et démocratie », in « Transparence et secret », *Pouvoirs*, 2001.

[3] J.M. Sauve, « Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? », in *Transparence, valeurs de l'action publique et intérêt général*, Colloque organisé par *Transparency International*, Assemblée Nationale, Paris, 5 mai 2011.

2. Avant d'aborder les différents angles, par lesquels le droit approche ce conflit entre « Ombres et Lumières », nous proposons un bref commentaire sur les relations qu'entretient le numérique avec les concepts de transparence et de secret. Dans le texte cité ci-dessus, Sauvé affirme que les technologies de l'information et de la communication constituent le vecteur d'une plus grande transparence de nos sociétés. L'affirmation nous apparaît valide en grande partie et ce pour trois raisons :

– la technologie est de plus en plus ubiquitaire : elle envahit nos vies, piste nos déplacements, enregistre nos comportements même les plus triviaux de *surfing*, de consommation, dévoile nos sentiments et demain reconstruira nos personnalités. Bref, la technologie nous rend transparent et prétend grâce à cette transparence mieux nous servir et guider. Les différentes technologies permettent la collecte d'une information qualitativement et quantitativement de plus en plus diverse et riche à laquelle les traitements d'intelligence dite artificielle apportent une indéniable valeur ajoutée. Pour faire bref, si la technologie nous rend transparents, il n'est pas sûr, par contre, qu'elle le soit pour nous ;
– la deuxième souligne les capacités décuplées de communication de nos messages et de diffusion de nos savoirs, ce qui incontestablement contribue à la transparence des événements, de leurs acteurs et de nos réflexions ;
– corrélativement – et c'est la troisième raison – l'accès à ces messages et à ces savoirs est chaque jour facilité : que l'on songe aux réseaux sociaux, aux moteurs de recherche dont les capacités de réaction et de découverte sont infinies ;

3. Pour autant, et dans le même temps, d'autres technologies favorisent la restriction de l'accès à l'information, ainsi les technologies de contrôle d'accès et le cryptage de messages enferment, mieux que dans un coffre-fort, nos secrets. Les technologies d'anonymat nous permettent de circuler sur le Net incognito et les méthodes dites de pseudonymat permettent de taire aux non-initiés notre identité. En d'autres termes, si le numérique favorise indéniablement la transparence, certaines de ses technologies entendent garantir nos secrets. Il faudra donc s'interroger sur les complicités que le droit peut entretenir avec la technologie tantôt pour renforcer la transparence, tantôt pour la restreindre. Notre interrogation se précise : pourquoi et pour qui, le droit fera-t-il alliance avec la technologie pour favoriser la transparence ? Pourquoi et pour qui le droit demandera-t-il aux technologies de protéger nos zones d'ombre ?

4. Ces questions nous amènent à des réponses différentes suivant les thèmes abordés. Nous en proposons cinq, que nous considérons comme essentiels dans ce débat.

– L'accès aux documents administratifs et de manière plus générale, à l'information détenue par les autorités publiques et ce au nom de la transparence, au service elle-même de la démocratie. Sauf exceptions limitées, le droit se met en la matière au service de la transparence en vue d'assurer un fonctionnement démocratique de nos sociétés. Dans un environnement technologique, en quoi le droit peut-il s'appuyer sur ces dernières pour atteindre cet objectif démocratique ?
– La protection des données : à l'heure où les technologies de la communication autorisent une quasi-transparence unilatérale des personnes concernées face aux responsables de traitement, le droit entend en s'appuyant sur ces mêmes technologies limiter cette transparence et offrir aux personnes concernées une certaine réciprocité dans cette transparence. Au-delà, il importe que le droit maintienne des lieux de secret et un droit à l'anonymat.
– Le secret professionnel : consacrée par le droit pénal, la protection des secrets professionnels s'effrite au gré de l'utilisation de plus en plus grande du numérique par les professionnels.
– Les régimes de dénonciation et de collaboration avec l'administration : le contrôle sociétaire des déviances du comportement d'autrui est encouragé, il devient un devoir moral voire une obligation juridique au service d'une société transparente où chacun s'autorise et est autorisé à surveiller son voisin. La directive récente sur les lanceurs d'alerte doit être étudiée dans cette perspective.
– Enfin, le droit de la propriété intellectuelle s'appuie sur le numérique pour renforcer les secrets de la création et permettre une commercialisation des œuvres plus sécurisée et plus rentable. La récente directive européenne sur les secrets d'affaires crée une sorte de droit sui generis qui protège l'entreprise du regard des concurrents et des « fuites » des employés. La récente directive dite *Copyright Act in an Information Society* accroît encore les prérogatives des auteurs ou plutôt de leurs ayants droit et confie aux plateformes de communication et d'information un rôle important dans la lutte contre les copies. À l'inverse, des mouvements citoyens trouvent dans le même droit de la propriété intellectuelle la possibilité de profiter du numérique pour assurer un large accès aux œuvres et logiciels. C'est tous les mouvements dits d'*open data, d'open source ou d'open document.*

5. Qu'on en juge… droit et technologie s'allient ou peuvent s'allier, se combattent ou peuvent se combattre tantôt dans le sens d'une plus grande transparence, tantôt pour mieux protéger le secret. Quelle combinaison proposer ? Sans doute, au-delà de ce que le juriste peut proposer, il y a lieu de tenir un débat sociétaire autour de principes éthiques avant que nos instances démocratiques ne décident.

CHAPITRE 1. De la transparence des décideurs publics à l'ère du numérique

6. L'origine des exigences de transparence du fonctionnement de l'État et des autorités publiques remonte, certes, au début du XX^e^ siècle comme le rappelait un article récent de Joassart[4]. Sa traduction réglementaire est cependant plus récente. Basée sur l'article 10 de la convention du Conseil de l'Europe, la Recommandation n° R(81) 19 du Comité des ministres aux États membres du Conseil sur l'accès à l'information détenue par les autorités publiques[5] justifiait son intervention par la nécessité dans une société démocratique, où chacun dispose de la liberté d'expression, de permettre à chacun de pouvoir connaître et critiquer l'action et les décisions des autorités publiques et de pouvoir dès lors participer aux processus de

[4] M. JOASSART, « Le secret en droit administratif », in *Le secret*, coll. Recyclage en droit, vol. 4, Limal, Anthemis, 2017, p. 7, citant M. HAURIOU : « la conscience moderne exige que l'administration agisse au grand jour. On lui a longtemps toléré des décisions secrètes. Maintenant, on veut que toutes ses décisions et toutes ses actions soient publiques et l'on a le sentiment que ce qui n'a pas été fait publiquement n'est pas régulier ».

[5] Aujourd'hui, ce droit à l'information est considéré comme une exigence du droit international par l'UNESCO : « Le Droit d'accès à l'information (DAI) est un droit fondamental de l'individu et de la collectivité de chercher à savoir et de faire savoir ce qui se passe dans la vie publique. Les lois relatives à la liberté d'information reflètent le postulat essentiel selon lequel toutes les informations détenues par les gouvernements et les institutions gouvernementales sont en principe publiques et ne peuvent être cachées que s'il existe des raisons légitimes de le faire, les cas typiques étant le respect de la vie privée et les questions de sécurité par exemple. Au cours de ces dix dernières années, le droit à l'information a été reconnu par un nombre croissant de pays, à travers l'adoption d'un ensemble de lois sur le sujet. En 1990, ils n'étaient que 13 à s'être dotés de lois nationales relatives à la liberté d'information, alors qu'on compte aujourd'hui 94 législations semblables dans le monde ».

décision.[6] Depuis, la Convention du Conseil de l'Europe[7] en établit plus fermement encore le principe : « Estimant que l'exercice du droit d'accès aux documents publics : fournit une source d'information au public ; aide le public à se former une opinion sur l'état de la société et sur les autorités publiques ; favorise l'intégrité, le bon fonctionnement, l'efficacité, et la responsabilité des autorités publiques contribuant ainsi à affirmer leur légitimité… Chaque Partie garantit à toute personne, sans discrimination aucune, le droit d'accéder, à sa demande, à des documents publics détenus par des autorités publiques… ». L'Union européenne adopte vis-à-vis de ses organes et autorités la même règle[8] et la Belgique, comme d'autres pays, a traduit le prescrit dans l'article 24*ter* de la Constitution (devenu, après la coordination de la Constitution, l'article 32) et dans une série de lois fédérale, régionales et communautaires[9]. Depuis, on note que l'obligation de transparence s'étend non seulement aux contenus des décisions et de l'action administrative ou gouvernementale mais, également, s'entend des avoirs et positions des acteurs publics[10] et de la qualité de ceux qui entourent la prise de décisions publiques : les lobbyistes[11].

7. Certes, l'article 32 de la Constitution ne consacre pas une transparence totale de l'administration. Le droit à la transparence cède, suivant les différents textes législatifs européens ou nationaux cités, lorsque priment la liberté d'autrui (sa vie privée), l'intérêt général supérieur de l'État (secret d'État, politique monétaire…) ou le secret des délibérations, nécessaires à la qualité de cette délibération[12]. Bref, la transparence s'arrête là

---

[6] Parmi de nombreux auteurs à propos des textes du Conseil de l'Europe, F. EDEL, « La convention du conseil de l'Europe sur l'accès aux documents publics : premier traité consacrant un droit général d'accès aux documents administratifs », in *Revue française d'administration publique*, 2011, pp. 57 et s.

[7] Convention du Conseil de l'Europe sur l'accès aux documents publics, Traité du 18 juin 2009, n° 205.

[8] Règlement n° 1049/2001.

[9] Sur l'ensemble de ces textes et sur la portée de l'article 32 de la Constitution, lire C. DE TERWANGNE, « Le droit à la transparence administrative », in M. VERDUSSEN et N. BONBLED (dir.), *Les droits constitutionnels en Belgique*, t. 2, Louvain-la-Neuve, Academia/Bruylant, 2010, pp. 703-744.

[10] Voy. sur le site CUMULEO (www.cumuleo.be) la liste impressionnante des acteurs publics tenus, par la loi du 2 mai 1995 et celles qui lui ont fait suite, d'une déclaration patrimoniale auprès de la Cour des comptes, accessible au public.

[11] Ainsi, le règlement européen du 22 novembre 2016 relatif aux activités de lobbying.

[12] L'article 3 de la Convention du Conseil de l'Europe établit ainsi la liste des exceptions possibles : « Chaque Partie peut limiter le droit d'accès aux documents publics. Les limitations sont établies précisément dans la loi, nécessaires dans une société démocratique et proportionnelle au but de protéger :

a. la sécurité nationale, la défense et les relations extérieures ;

où s'affirme la nécessité prédominante du secret. On connaît la tendance de la jurisprudence à restreindre les exceptions aux seules hypothèses où l'atteinte au droit à la transparence n'est pas *in casu* jugée excessive : « En permettant qu'un législateur puisse prévoir dans quels cas et à quelles conditions il peut être dérogé au principe de la transparence administrative, le Constituant n'a pas exclu que l'accès à certains documents soit soumis à des conditions ou soit limité, pour autant que ces restrictions soient raisonnablement justifiées et n'entraînent pas d'effets disproportionnés. Il convient, à cet égard de souligner que la transparence administrative participe à l'effectivité de l'exercice du droit de recours des administrés devant le Conseil d'État ou devant les juridictions judiciaires »[13]. Cette tendance à l'interprétation restrictive des exceptions justifie l'obligation mise à charge de l'État en cas de refus de divulgation de démontrer en quoi la révélation de l'information couverte par le secret met en péril l'intérêt protégé par cette exception ? et ce, même dans les cas où l'exception de secret est dite « absolue »[14].

8. Que dire de l'influence du numérique en ce qui concerne cette obligation de transparence ? Notre introduction attestait combien le numérique facilite la diffusion et la communication des données tout en limitant sévèrement les coûts de celles-ci. Bref, il est tentant d'obliger les administrations à utiliser les technologies de l'information et de la communication au service d'une administration désormais plus transparente. À cet égard, à la suite du conseiller d'État Sauve, on reprendra les propositions du rapport public du Conseil d'État français de 2011 : « Consulter autrement, participer effectivement ». Ce rapport examine comment grâce au numérique, il est possible de dégager de nouveaux principes

b. la sûreté publique ;
c. la prévention, la recherche et la poursuite des activités criminelles ;
d. les enquêtes disciplinaires ;
e. les missions de tutelle, l'inspection et le contrôle par l'administration ;
f. la vie privée et les autres intérêts privés légitimes ;
g. les intérêts commerciaux et d'autres intérêts économiques ;
h. la politique économique, monétaire et de change de l'État ;
i. l'égalité des parties à une instance juridictionnelle et le bon fonctionnement de la justice ;
j. l'environnement ; ou
k. les délibérations au sein de ou entre les autorités publiques concernant l'examen d'un dossier ».

[13] C. const., 19 décembre 2013, n° 169/2013, *A.P.T.*, 2014, pp. 576 et s. ; note D. Renders et G. Charpentier.

[14] Voy. sur ce point, les nombreuses références aux décisions des Commissions dites d'accès aux documents administratifs (CADA) et du Conseil d'État, décisions citées par M. Joassart, « Le secret en droit administratif », *op. cit.*, pp. 14 et s.

directeurs de la prise d'une décision dans le cadre d'une administration dite « délibérative ». Ainsi, « figurent, notamment, l'accessibilité des informations publiques, l'obligation de diffusion des observations de tous les participants à des procédures de consultation, l'impartialité et la loyauté de ces procédures par la mise en place éventuelle d'un "tiers garant" et l'obligation pour l'administration de rendre compte des suites données à ses consultations ».

Notons d'abord que le numérique permet une modernisation et une meilleure effectivité du droit d'accès. Introduire sa demande d'accès via un simple portail électronique qui, le cas échéant, garantira l'anonymat du demandeur, obliger l'administration à répondre par la voie électronique et selon le format réclamé par la personne concernée apparaissent comme une évolution évidente du droit d'accès dans le contexte d'une société dite du numérique[15]. Sans doute, peut-on imaginer aller plus loin et réclamer que l'accès à l'information ne soit plus à une information brute mais s'étende à l'information liée. Ainsi, ma demande d'accéder aux noms des administrateurs d'une société peut s'accompagner d'une demande sur les prédécesseurs ou d'une information sur les autres sociétés dont les administrateurs recherchés sont également administrateurs. Réclamer de connaître le détail des dépenses budgétaires de telles communes se conçoit également d'une information sur les dépenses des années précédentes. Ajoutons que la gestion numérique temporelle (*Audit Trail)* des dossiers à l'intérieur de l'administration permettrait – et certains législateurs l'ont déjà imposé- aux administrés de suivre l'évolution de leurs dossiers au sein de l'administration et de garantir ainsi la transparence du processus administratif[16]. Connaître en temps réel la situation de son dossier, le parcours déjà accompli et celui restant à accomplir, les autorisations obtenues, celles encore à obtenir constituerait un bénéfice incontestable que le numérique peut apporter à la transparence de l'administration vis-à-vis des citoyens.

---

[15] L'Electronic Freedom Information Act américain (US E-FOIA) contient de telles extensions. « *The Electronic Freedom of Information Act Amendments of 1996 (E-FOIA) stated that all agencies are required by statute to make certain types of records, created by the agency on or after November 1, 1996, available electronically. Agencies must also provide electronic reading rooms for citizens to use to have access to records. Given the large volume of records and limited resources, the amendment also extended the agencies' required response time to FOIA requests. Formerly, the response time was ten days and the amendment extended it to twenty business days* » (Wikipédia). Sur l'E-FOIA, lire C. Lamouline et Y. Poullet, *Des autoroutes de l'information à la "démocratie électronique" : de l'impact des technologies de l'information et de la communication sur nos libertés*, Bruxelles, Bruylant/Nemesis, 1997.

[16] Sur ce développement possible de la transparence administrative, qu'elle fonde sur le droit d'accès conféré par les lois de protection des données, lire E. Degrave, *L'e-gouvernement et la protection des données*, Bruxelles, Larcier, 2013, pp. 467 et s.

9. L'apport du numérique à la diffusion des informations justifie – faut-il le dire – un plaidoyer fort en faveur de la publicité active de l'administration et non un simple renforcement de la publicité passive. C'est que l'autorité publique a le devoir de mettre à disposition des citoyens, d'initiative (publicité active) et non dans les seuls cas d'une démarche du citoyen (publicité passive), toute information dont la connaissance est jugée par l'autorité comme d'intérêt général. Dès 1996, nous plaidions pour la reconnaissance d'un service universel d'informations publiques[17]. Il s'agissait, à partir de l'analyse de la situation et des besoins sociaux d'une population voire d'acteurs économiques, qu'au nom de considérations d'intérêt général soit établi un service universel d'informations publiques, c'est-à-dire un service répondant aux caractéristiques suivantes :

– l'universalité, c'est-à-dire l'accès pour tous les usagers à des conditions abordables ;
– l'égalité des usagers, c'est-à-dire l'accès non discriminatoire ;
– la continuité, c'est-à-dire la garantie d'une offre de services continue, selon une qualité définie.

De nombreux exemples que ce soit en matière culturelle (richesse des musées), de transports (impacts de travaux sur l'infrastructure), d'enseignement (présentation des institutions, de l'évolution des chiffres…), de politique scientifique, etc. peuvent être donnés[18]. Sans doute, cette reconnaissance intéresse les entreprises qui convoitent les richesses informationnelles publiques dans la mesure où la connexion de ces informations avec d'autres informations et/ou leur structuration via les logiciels qu'ils détiennent, permet aux entreprises d'offrir des services à valeur ajoutée. Une telle considération expliquait la directive européenne 2003/98 prise dès le 17 novembre 2003 sur la réutilisation des données du secteur public[19]. Elle pourrait, dans le cadre du développement des initiatives locales de *Smart Cities*, s'étendre à un devoir pour les autorités locales de

[17] Y. Poullet, « Vers un ou des services universels d'informations publiques », in *Access to Public Information A Key to commercial Growth and Electronic Democracy*, Colloque organisé par la Commission européenne dans le cadre d'INFO 2000, Stockholm, 26/27 juin 1996, disponible sur http://www.echo.lu/legal/stockholm/fr/poullet.html.

[18] On se référera sur ce point au rapport de P. Canavaggio, *Vers un droit d'accès à l'information publique*, publié par l'UNESCO, 2014 et l'intérêt des ONG au développement de cette politique.

[19] Directive modifiée par la directive 2013/37/UE du Parlement européen et du Conseil du 26 juin 2013 et concernant la réutilisation des informations du secteur public. Les considérants de la directive de 2013 insistent sur la nécessité de tenir compte des opportunités nouvelles qu'offre la numérisation y compris dans le domaine culturel : « La numérisation constitue un moyen important de renforcer l'accès au matériel culturel et la réutilisation de

mettre à disposition, cette fois, des simples citoyens les données qui correspondent à l'intérêt général local comme des informations sur les travaux locaux, des statistiques sur l'évolution de la population locale, sur les institutions d'enseignement, etc. Enfin, elle pourrait s'étendre aux entreprises elles-mêmes dont la puissance économique et le poids sociétaire pourraient amener le législateur à exiger qu'elles rendent des comptes en ce qui concerne des informations essentielles pour notre société[20].

10. À propos de l'accès aux documents publics et, de manière plus large, du devoir de transparence des autorités publiques mais également de certaines entreprises privées, on soulignera diverses interventions réglementaires européennes. La première est certes la décision du « trilogue » européen (Commission, Parlement, Conseil des ministres) prise le 22 janvier sur le texte de révision de la directive PSI[21]. Cette révision élargit le champ d'application de la directive actuelle à certaines entreprises publiques, accentue le devoir des États d'offrir, avec des contraintes minimales tant légales, financières que techniques, les données en « open data », en particulier les bases de données qui présentent une haute valeur ajoutée au marché de l'information. Il est clair que la principale préoccupation de la modification est la volonté européenne de créer un vaste marché de l'information digitale comme le note l'accord du 22 janvier : « *Data is the fuel that drives the growth of many digital products and services. Making sure that high-quality, high-value data from publicly funded services is widely and freely available is a key factor in accelerating European innovation in highly competitive fields such as artificial intelligence requiring access to vast amounts of high-quality data* »[22]. La même volonté de créer un marché commun de l'information expliquait l'idée défendue par la Commission d'un

celui-ci, à des fins éducatives, professionnelles ou de loisirs. Elle offre également d'importants débouchés économiques, en facilitant l'intégration du matériel culturel dans les services et produits numériques, concourant ainsi à la création d'emplois et à la croissance ».

[20] Les obligations pour les entreprises de publier les comptes annuels à la banque nationale et certaines informations dues notamment en matière d'environnement ou en matière de *privacy policy*, constituent déjà de premières manifestations sur ce devoir de transparence des autorités « privées ». On note plus récemment la proposition de la Commission européenne de rendre publics certains éléments de la déclaration pays par pays (*Country-By-Country Report*) : Proposition de directive du Parlement européen et du Conseil modifiant la directive 2013/34/UE en ce qui concerne la communication, par certaines entreprises et succursales, d'informations relatives à l'impôt sur les bénéfices, 12 avril 2016, COM(2016) 198 final.

[21] Proposition de directive pour une révision de la directive PSI, publiée à l'adresse https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive

[22] On notera en outre que lors des discussions, il avait un moment été envisagé un *reverse PSI*, c'est-à-dire l'obligation des entreprises privées de transférer des données au secteur public de manière çà permettre à ce dernier de disposer d'informations plus complètes et de définir ainsi de meilleures stratégies d'action par exemple en mobilité, énergie…

reverse PSI[23], soit l'obligation cette fois pour les entreprises privées détentrices de données d'utilité générale de devoir, certes moyennant rémunération, mettre certaines de leurs données à disposition de l'État. Ainsi, on peut imaginer l'intérêt du public de pouvoir, grâce à la géolocalisation permise par les logiciels insérés dans nos mobilophones, de connaître les habitudes de déplacement des citoyens, les lieux et moments des bouchons routiers, de découvrir les progressions d'épidémie que révèlent les interrogations sur les moteurs de recherche, etc. Finalement, devant les protestations, en particulier des plateformes de communication et d'information, la Commission européenne renonce le 25 avril 2019 à imposer ce devoir aux entreprises mais se contente d'une recommandation de traitement préférentiel de leur part à l'égard des pouvoirs publics.

11. La directive du 20 juin 2019 dite *Open Data*[24] note : « Les informations du secteur public constituent une source extraordinaire de données qui peuvent contribuer à améliorer le marché intérieur et à développer de nouvelles applications pour les consommateurs et les personnes morales. L'utilisation intelligente de données, y compris leur traitement par des applications utilisant l'intelligence artificielle, peut avoir un effet de transformation sur tous les secteurs de l'économie » (consid. n° 9). Pour ce faire, elles recommandent aux autorités et entreprises publiques de mettre en format ouvert les données dont elles disposent : « les organismes du secteur public et les entreprises publiques mettent leurs documents à disposition dans tout format ou toute langue préexistants et, si possible et s'il y a lieu, sous forme électronique, dans des formats qui sont ouverts, lisibles par machine, accessibles, traçables et réutilisables, en les accompagnant de leurs métadonnées. Tant le format que les métadonnées répondent, autant que possible, à des normes formelles ouvertes[25] » (art. 5.1).

12. Deux décisions récentes, l'une de la Cour de justice de Luxembourg, l'autre de la Cour du Conseil de l'Europe, toutes deux à propos de la publication de données à caractère personnel amènent à nous interroger : les

[23] « Towards a common European data space », Communication de la Commission, Brussels, 25 avril 2018 COM(2018) 232 final.

[24] Directive 2019/1024/UE du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public, *J.O.U.E.*, 20 juin 2019, L.172/56.

[25] Le même article en son alinéa 8 rend la recommandation obligatoire « en ce qui concerne les ensembles de données de forte valeur, dont la liste est établie conformément à l'article 14, paragraphe 1, sont mis à disposition à des fins de réutilisation dans des formats lisibles par machine, en recourant à des API appropriées et, le cas échéant, sous la forme d'un téléchargement de masse ».

potentialités que le numérique offre aux bénéficiaires du droit d'accès à l'information n'amènent-elles pas à devoir réfléchir à une remise en cause de l'approche restrictive des exceptions, développée ci-avant ? Dans l'affaire *Google c. Spain* tranchée le 13 mai 2014 par la Cour de justice des communautés européennes[26], il est reproché à Google de mettre son moteur de recherche au service de la recherche d'informations pourtant publiques relatives au jugement portant sur un particulier. Dans la seconde *Satakunnan c. Finlande* jugée le 27 juin de cette année, cette fois par la Cour de Strasbourg[27], il est reproché à une entreprise en concertation avec un éditeur de journaux d'offrir un service aux citoyens d'interroger une base de données nourrie en grande partie par des informations obtenues dans le cadre de la loi d'accès aux documents administratifs et portant sur la situation fiscale de chaque contribuable finlandais. Les questions soulevées par ces deux arrêts sont nombreuses. On en relève deux. La première s'interroge sur la qualité de l'offreur de services, Google, d'un côté, l'entreprise offrant un service à valeur ajoutée comme sous-traitant de l'éditeur de journaux, peut-on les considérées comme participant à une activité journalistique qui selon l'article 85 du règlement bénéficie d'un régime particulier destiné à concilier le droit à la liberté d'expression et le droit à la protection des données ? La Cour européenne de Luxembourg rejette sans autre forme de discussion la qualification d'activités journalistiques aux services de Google, au motif que leur visée est d'abord économique[28] ; de manière moins tranchée et nonobstant deux opinions dissidentes, la Cour de Strasbourg met en doute le fait que l'activité d'une entreprise même journalistique ait, au vu de l'exploitation numérique des données, pour *seules* fins le journalisme « dans la mesure où la publication litigieuse ne saurait passer pour contribuer à un débat d'intérêt général… »[29]. La seconde a été de peser l'intérêt des personnes concernées mis

[26] Affaire *Google*, C 131/12.

[27] Arrêt de la Cour européenne des droits de l'homme (GC), affaire *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*, requête n° 931/13, 27 juin 2017.

[28] *Cf.* consid. n° 85 de l'arrêt *Google c. Spain* : « En outre, le traitement par l'éditeur d'une page web, consistant dans la publication d'informations relatives à une personne physique, peut, le cas échéant, être effectué « aux seules fins de journalisme » et ainsi bénéficier, en vertu de l'article 9 de la directive 95/46, de dérogations aux exigences établies par celle-ci, tandis que tel n'apparaît pas être le cas s'agissant du traitement effectué par l'exploitant d'un moteur de recherche. Il ne peut ainsi être exclu que la personne concernée soit, dans certaines circonstances, susceptible d'exercer les droits visés aux articles 12, sous b), et 14, premier alinéa, sous a), de la directive 95/46 contre ledit exploitant, mais non pas contre l'éditeur de ladite page web ».

[29] Consid., n° 175 : « la publication des données fiscales selon les modalités et à l'échelle en question n'avait pas contribué à un débat d'intérêt général et que les sociétés requérantes ne pouvaient pas prétendre, en substance, que cette activité de publication avait été

en cause par la publication et celui de l'éditeur et des tiers. Sur ce point, dans l'affaire *Google*, les juges luxembourgeois estiment que « l'inclusion dans la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, d'une page web et des informations qui y sont contenues relatives à cette personne facilite sensiblement l'accessibilité de ces informations à tout internaute effectuant une recherche sur la personne concernée et peut jouer un rôle décisif pour la diffusion desdites informations, elle est susceptible de constituer une ingérence plus importante dans le droit fondamental au respect de la vie privée de la personne concernée que la publication par l'éditeur de cette page web. »[30]. Sur cette base, il est jugé[31] que « ces droits (ceux de la personne concernée) prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne ». Dans l'affaire finlandaise, les juges strasbourgeois estiment de même que « l'accessibilité des données en question au public en vertu du droit interne ne signifie pas nécessairement qu'elles pouvaient être publiées sans aucune restriction. La publication des données dans un magazine et leur diffusion ultérieure au moyen d'un service SMS les ont rendues accessibles selon des modalités et à une échelle qui n'étaient pas prévues par le législateur »[32]. Ainsi, les risques nouveaux créés par l'utilisation des technologies de l'information par les bénéficiaires du droit

---

exercée aux seules fins de journalisme au sens de la législation nationale et européenne ». Cinq critères sont rappelés qui permettent de bénéficier de l'exception de journalisme « (i) la contribution de la publication au débat d'intérêt général (ii) l'objet de la publication et la nature des personnes concernées (iii) la façon dont l'information a été obtenue et la véracité de celle-ci (iv) le contenu, la forme et les conséquences de la publication et, enfin (v), la sanction » (K. LEMMENS, « La liberté d'expression à l'heure d'Internet », in *L'Europe des droits de l'homme à l'heure d'Internet* (C. de TERWANGNE et Q. VAN ENIS dir.), Bruxelles, Bruylant, 2019). À noter à l'inverse, la définition très (trop) large donnée à cet égard à la notion de « media d'informations » (soit d'entreprise journalistique) par l'Open Government Act US de 2007 : « *it recognizes electronic media specifically and defines "News Media" as "any person or entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience* ».

[30] Consid. n° 87.

[31] Consid. n° 97. Les juges ajoutent : « Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question ».

[32] Consid. n° 190 voy. aussi, les conclusions, n° 196. On opposera à ce raisonnement, l'opinion minoritaire exprimée par deux juges strasbourgeois qui rejettent les restrictions ainsi faites aux activités journalistiques et considère qu'il n'existe aucun intérêt à garder secrètes des informations dont le contenu avait été rendu public et était susceptible d'être connu par un grand nombre de personnes.

d'accès devraient amener les administrations[33] à prévoir des restrictions quant à l'utilisation des données à caractère personnel ainsi obtenues. L'article que nous signons avec Thierry Léonard présent dans cette publication revient longuement sur ce débat.

13. Enfin, le numérique modifie la façon de décider de l'administration, celle-ci utilisant de plus en plus des systèmes d'intelligence artificielle pour calculer les droits des administrés. Nous reviendrons sur ce point dans la mesure où les lois de protection des données ouvrent aux personnes concernées en l'occurrence les administrés certains droits nouveaux en la matière (*infra*, n° 16). Notons simplement à la suite de M. Gerard, que « le droit fondamental d'accès à l'information détenue par les autorités administratives devrait s'entendre 'des informations concernant entre autres, le rôle dévolu à l'intelligence artificielle au sein de l'administration, la manière dont elle est supervisée par des fonctionnaires 'humains', les types de décisions qu'elle peut prendre, la manière dont ces décisions sont prises… »[34]. On ajoutera à la suite de la décision des autorités communales de New York, que l'accès en langage compréhensible au code source des logiciels d'intelligence artificielle devrait être garanti afin de permettre aux citoyens de connaître la logique sous-tendant la décision prise à son égard.

CHAPITRE 2. De la transparence… et du secret : les lois de protection des données

14. La technologie du numérique est chaque jour plus ubiquitaire. Elle accompagne chacune de nos actions, demain de nos pensées ; les capacités de nos systèmes d'information explosent, les applications se multiplient et s'enrichissent de données toujours plus nombreuses dont nous sommes consciemment ou inconsciemment les principaux émetteurs. Ces données sont collectées de plus en plus à partir d'objets autour de nous voire en nous et stockées « dans les nuages ». Les corrélations entre ces données autorisent des profilages dont la finalité est souvent sécuritaire ou

[33] On regrette que dans l'affaire *Google*, ces restrictions reposent non sur l'administration source de l'information mais sur le prestataire privé (Google) et oblige celui-ci à mettre en balance l'intérêt à savoir et celui au secret.

[34] L. Gerard, « Robotisation des services publics : l'intelligence artificielle peut-elle s'immiscer sans heurt dans nos administrations ? », in H. Jacquemin et A. de Streel (ed.), *L'intelligence artificielle et le droit*, coll. du CRIDS, n° 41, Bruxelles, Larcier, 2017, p. 434.

commerciale et permettent, face à l'insécurité des comportements, de préempter les actions des individus voire de les manipuler[35]. Ces potentialités du numérique créent le risque bien réel d'une transparence unilatérale des « personnes concernées », vis-à-vis des « responsables de traitement » comme les qualifient les lois de protection des données. La situation renvoie à l'image du *Big Brother* d'Orwell, soit d'un pouvoir informationnel détenu par les « Information haves », en particulier les GAFA[36] vis-à-vis des citoyens ou simples consommateurs, démunis faute de savoir ce que les premiers connaissent d'eux. Cette situation renvoie à une seconde image, celle du prisonnier décrit par le roman *Trial* de Kafka où ce prisonnier ignorant les raisons de son emprisonnement perd peu à peu sa personnalité vis-à-vis de son juge et de ses policiers, cherchant à anticiper le comportement qu'il croit attendu par eux[37]. Comme le note le tribunal constitutionnel de Karlsruhe dans sa décision déjà ancienne de 1983 relative à la loi sur le recensement[38], cette opacité des traitements entraîne de la part des citoyens un conformisme anticipatif des comportements, ce qui est le contraire de la démocratie qui exige des hommes et femmes libres et capables d'auto-détermination.

En réponse à cette transparence unilatérale, les lois de protection des données entendent, d'une part, limiter le droit des responsables de traitement à utiliser le numérique dans leur quête de transparence et, d'autre part, établissent, par la création de droits nouveaux au bénéfice

---

[35] On connaît la phrase du CEO de Google : « *It will become very difficult for people to see or consume something that has not in some sense been tailored for them* ». Sur les différentes techniques utilisées par les entreprises pour influencer leurs « clients », lire l'excellent ouvrage de vulgarisation, H. Bersini, *Big Brother is driving you*, Académie royale de Belgique, coll. L'académie en poche, 2018.

[36] Acronyme reprenant les premières lettres des 4 sociétés les plus actives sur le marché de services du numérique, soit Google, Amazon, Facebook et Apple. Il est coutumier depuis la création de l'acronyme d'ajouter Microsoft et Ali baba (société chinoise).

[37] Le lecteur trouvera dans notre ouvrage (Y. Poullet, *La vie privée à l'heure de la société du numérique – Essai*, Cahier du Crids, n° 45, Bruxelles, Larcier, 2019) des développements complets sur les risques du numérique et les deux figures qui permettent de les approcher.

[38] « *The possibility of inspection and of gaining influence have increased to hitherto unknown, and may influence the individuals'behaviour by the psychological pressure exerted by public(or private) interests. Even in certain conditions of modern information processing technology, individual self-determination presupposes that the individuals left with the freedom of decision about actions to be taken or to be omitted, including the possibility to follow that decision in practice. If someone cannot predict with sufficiently certainty which information about himself in certain areas is known and cannot sufficiently estimate the knowledge of parties to whom communications may be possible, he is crucially inhibited in his freedom to plan or to decide freely… This would not only impact his chances of development but would have also impact the common good because self-development is an elementary functional condition of a free democratic society based on its citizen's capacity to act and cooperate* » (traduction libre).

des personnes concernées, une réciprocité dans la transparence. Au-delà, ces mêmes législations consacrent, sans doute de manière limitée et non absolue mais de manière certaine, le droit au secret. Étudions chacun de ses axes directeurs à travers les dispositions du récent règlement européen de protection des données[39].

15. Le **premier axe** porte sur les limites des traitements et le comportement responsable de ceux qui en tirent bénéfice. À cet égard, le règlement renforce les limites du droit au traitement. La question de la licéité du traitement est résolue de manière plus drastique qu'elle ne l'était sous la directive. Le consentement peut être retiré à tout moment. À défaut de consentement ou d'un autre fondement légal, le traitement est licite seulement lorsqu'il « est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel ». Cette pesée des intérêts tiendra compte, selon la jurisprudence des autorités de contrôle, des finalités du traitement, de la nature des données traitées, des attentes raisonnables des personnes concernées, du statut de la personne concernée et du déséquilibre de pouvoir informationnel qui peut exister entre le responsable et la personne concernée. Le principe de pertinence, qui préside à cette pesée d'intérêts, se voit précisé par un principe dit de minimisation : les données traitées doivent être limitées dans leur nombre et leur durée de traitement « à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Ce double principe implique que le responsable du traitement anonymisera les données ou utilisera de techniques de « pseudonymisation », chaque fois qu'il ne peut être démontré le besoin de recourir à des données à caractère personnel.

Le principe d'intégrité et de confidentialité est énoncé de manière très large : les données doivent être « traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction

[39] Sur ce règlement, désormais en vigueur depuis le 25 juin 2018, on renvoie le lecteur à l'ouvrage collectif du CRIDS : *Le règlement général sur la protection des données (RGPD/GDPR)* (C. DE TERWANGNE et K. ROSIER dir.), coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018. *Cf.* également d'autres commentaires, in *Data Protection : l'impact du GDPR en assurances* (C.A. van OLDENEEL ed.), Bull des assurances, Dossier Wolters Kluwer, 2017. *Cf.* également, deux articles, C. TIKKINEN-PIRI, A. ROHUNEN et J. MARKULLA, « EU GDPR : Changes and implication for personal Data collecting companies », *CL&SR*, 2017, C. DE TERWANGNE, K. ROSIER et B. LOSDYK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 62, 2016, pp. 5-56 et au commentaire de la CNIL, « Règlement européen sur la protection des données : Ce qui change pour les professionnels », 15 juin 2016, disponible sur le site de la CNIL (www.cnil.fr).

ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées ». Enfin, on ajoute que le § 2 de l'article 5 souligne le principe dit de responsabilité (*accountability*) : « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté ». En d'autres termes, l'article établit un renversement de la charge de la preuve : c'est au responsable du traitement à démontrer que, lors de la création et tout au long du traitement, il a pris toutes les précautions pour satisfaire aux exigences de licéité, loyauté, proportionnalité et de minimisation des données et a assuré la sécurité des traitements, sachant que les sanctions nouvellement instaurées sont considérablement plus sévères que sous l'ancien régime.

On s'arrêtera un instant sur un autre principe important consacré par le règlement et qui illustre bien l'affirmation suivant laquelle si la technologie est cause du problème, c'est également elle qui peut fournir la solution. Ainsi nombre de prescrits consacrent la nécessité d'utiliser des solutions techniques afin de prévenir les risques d'atteintes à la protection des données. L'exigence de *privacy by design*, de mesures techniques de sécurité adéquates, le recours à des mesures de certification des logiciels ou des produits utilisés constituent autant d'exemples de la façon dont le droit recourt au numérique pour assurer l'effectivité des obligations qu'il impose aux responsables de traitement.

16. Le **deuxième axe** concerne la consécration de nombre de nouveaux droits à la personne concernée dont l'objectif est d'assurer une **certaine réciprocité dans la transparence**. L'article 12 du règlement impose au responsable, en vertu du principe de transparence, principe cardinal du régime de protection des données[40], les modalités de communication des traitements qu'il opère. L'information doit être claire, concise, exprimée en termes clairs et simples, elle doit être facilement accessible, ainsi via la possibilité de cliquer sur une icône apparaissant sur la page consultée. Si les données sont collectées automatiquement, selon le principe de réciprocité des avantages, le responsable se doit de fournir l'information via les mêmes voies et de permettre de la même manière les demandes d'information[41]. La directive prévoyait une liste des informations que le responsable devait fournir à la personne concernée lorsque le premier

[40] Sur le principe de transparence en matière de protection des données, lire not. E. Degrave, « Transparence administrative et traitements de données à caractère personnel », note d'observation sous Cass., 14 février 2013, *R.D.T.I.*, n° 53/2013, pp. 56 et s. ; D. De Roy, C. de Terwangne et Y Poullet, « La convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K*, n° 2/2007, pp. 314-319.

[41] On note que l'article prévoit en son point 8 que la Commission européenne pourra préciser les modalités de communication des informations dues par l'opérateur.

collectait des informations directement auprès de ce dernier (ex : via un questionnaire mis sur le site web du responsable) ou indirectement (ex : via le GPS installé par le vendeur dans le véhicule de l'acheteur) : identité du responsable, finalités de la collecte, les destinataires des données, caractère obligatoire ou non de la fourniture des données, existence du droit d'accès et de rectification. À cette liste, le règlement ajoute de nombreuses informations[42] : ainsi, l'existence, le cas échéant, d'un délégué à la protection des données, l'intérêt légitime dont le responsable se prévaut, l'intention de transférer les données vers un pays tiers, le droit de retrait du consentement, la durée du traitement, l'existence ou non de procédures de décision automatisée, l'intention ou non de procéder à des traitements ultérieurs.

En ce qui concerne l'accès aux informations sur le traitement, on note que lorsque les données ne sont pas collectées auprès de la personne concernée, celle-ci a droit à disposer des mêmes informations et, en outre, d'une information sur la source des données la concernant. Le droit d'accès institué par la directive est par ailleurs élargi. Au-delà des informations minimales actuellement dues (les finalités du traitement, les catégories de données traitées et les destinataires), l'article 15 du règlement ajoute la durée du traitement, le droit de connaître de l'existence de flux transfrontières concernant ses données, le droit à la rectification ou à l'effacement des données, le droit de réclamation mais également « l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ». Le considérant n° 63 rappelle que ce devoir du responsable de communiquer la logique du traitement[43] qui permet la prise de décision automatisée ne peut contrevenir au droit d'auteur protégeant le logiciel ni au

[42] Mentionnons que la liste prévue par la directive n'était pas exhaustive.

[43] Ce qui risque en toute hypothèse d'être difficile lorsqu'il s'agit d'un système d'intelligence artificielle où à partir d'un algorithme de bas, le programme apprend par lui-même des données qui le nourrissent et entre lesquelles il « essaie » de manière aléatoire des corrélations pour cette base définir des profils ou décider d'actions. Sur cette difficulté, Th. Hoeren et M. Niehoff, « AI in Medical Diagnoses and the Right to Explanation », *EdpL*, 2018, n° 3, pp. 308 et s. ; A. Mantelero, *Artificial Intelligence and Data Protection : Challenges and Possible Remedies – Report*, Comité consultatif de la convention n° 108 du Conseil de l'Europe, 3 décembre 2018, T-PD(2018)09Rev ; G. Malgieri et G. Comande, « Why a Right to Legibility of Automated Decision – Making Exists in the GDPR ? », *International Data Privacy Law*, 2017, vol. 7, n° 4, pp. 243 et s. Sur quelques pistes de solution, notamment, High Level Group of experts on AI, *Ethics Guidelines for trustworthy AI systems*, décembre 2018, publié par la Commission après commentaires le 9 avril 2019, disponible sur le site : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

secret d'affaires dont bénéficie le responsable[44], il n'empêche que cette limitation ne peut conduire à un refus de donner tout élément sur cette logique et de communiquer les catégories de données prises en considération pour décider[45]. La communication des informations dues suite à une demande d'accès électronique suit en principe la même voie. En ce qui concerne le droit de rectification ou d'opposition, le règlement innove par la création de droits nouveaux : ainsi, il crée le droit à l'oubli sur lequel nous reviendrons (infra, n° 17) le droit à la portabilité des données. Enfin à propos du droit d'opposition, en particulier, il réglemente le « profilage ». À ce dernier propos, le règlement en son article 21 offre aux personnes concernées le droit de s'opposer au résultat de tels profilages même si le § 2 de cet article excepte les cas où de telles décisions trouvent leur fondement dans un contrat[46] ou dans le consentement explicite de la personne concernée et ajoute même l'hypothèse d'une autorisation légale moyennant des mesures appropriées[47]. Ces exceptions ne dispensent pas le responsable qui s'en réclame, de mettre œuvre « des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision ».

17. Le règlement entend prendre en compte le bénéfice des technologies nouvelles pour renforcer la protection de la personne concernée. Si effectivement les technologies nouvelles renforcent le pouvoir informationnel des responsables de traitement en permettant une collecte à distance des données relatives aux personnes concernées, en multipliant les données collectées tant dans leurs quantités que dans leurs qualités et natures et, enfin, en autorisant grâce à des algorithmes de plus en plus puissants, une connaissance des personnes concernées de plus en plus fine voire prédictive, il est normal d'exiger en retour une réciprocité des avantages du numérique : les mêmes technologies doivent pouvoir être

[44] Rappelons que le législateur européen a récemment adopté une directive visant à protéger spécialement le secret d'affaires au sein de l'union (directive 2016/943/UE du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.*, 15 mai 2016, L 157/1 à L 157/18).

[45] Cette obligation de fournir des informations sur l'algorithme utilisé dans les systèmes d'intelligence artificielle est fondamentale dans la mesure où elle permet aux personnes concernées ou à des associations les représentants de pouvoir contester « les vérités sorties de l'ordinateur ».

[46] Ce qui sera souvent le cas, ainsi dans le cadre d'opérations bancaires ou d'assurance.

[47] Le considérant n° 71 mentionne parmi ces « mesures », l'information spécifique des personnes concernées, le droit de la personne concernée à une intervention humaine, etc.

utilisées par les personnes concernées dans l'exercice de leurs droits et en permettre une meilleure effectivité. Il s'agit de rééquilibrer les intérêts respectifs en jeu. C'est en ce sens que le considérant n° 63 affirme que « des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés par le présent règlement… le responsable du traitement devrait également fournir les moyens de présenter des demandes (NDLA : d'accès, de retrait de consentement, de rectification, d'opposition, de recours…) par voie électronique, en particulier lorsque les données font l'objet d'un traitement électronique ». À nouveau, on souligne l'approche techno-légale, l'alliance du droit et de la technologie pour renforcer les droits des personnes concernées et en particulier la transparence des traitements.

18. Enfin, **troisième axe**, l'exigence de vie privée peut s'entendre de la garantie du maintien d'un secret. La garantie du secret ou en tout cas du non partage hors les cas de communications légitimes dérive des obligations de sécurité renforcées par le règlement et mises à charge des responsables de traitement, singulièrement des prestataires de services de communication[48]. À ce dernier propos, comme le note récemment le Contrôleur européen à la protection des données[49] à propos de la réforme souhaitée de la directive e-Privacy[50], le principe de la confidentialité des communications est essentiel et doit comprendre à la fois le contenu, les métadonnées et les données relatives à l'équipement terminal, il doit s'appliquer autant à des communications entre personnes qu'entre machines et couvrir le recours au *Cloud Computing*.

Le besoin de secret peut s'expliquer par l'écoulement du temps qui rend obsolète ou, plutôt, non pertinente la donnée traitée. Le droit

[48] On note également la directive 2016/1148 du 6 juillet 2016 sur le niveau élevé commun de sécurité des réseaux et des systèmes d'information. Cette directive exige de certaines entreprises assurant des services dits essentiels dans des secteurs critiques ou des services digitaux (*online marketplaces*, moteurs de recherches, *cloud computing*) de prendre des mesures de sécurité appropriées aux risques particuliers et de notifier les incidents à l'autorité nationale compétente.

[49] La directive *e-Privacy* a été adoptée dans un premier temps en 2002 (directive du 12 juillet 2002 concernant le traitement de données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques), elle a été modifiée profondément en 2009 et est actuellement en cours de révision comme l'a annoncé la Commission européenne dans son document *Digital Single Market Strategy* (6 mai 2015). En janvier 2017, la proposition de la Commission a été publiée.

[50] EDPS, *Recommendations on specific aspects of the proposed ePrivacy Regulation*, 5 octobre 2017, 2017, disponible sur le site de l'EDPS : www.edps.europa.eu.

à l'effacement ou droit à l'oubli[51] institué par l'article 18 du règlement offre ainsi la possibilité pour la personne concernée d'exiger la destruction[52], dans les meilleurs délais, des données le concernant dans certains cas dont l'énumération est évidente : inexistence ou retrait du consentement, opposition par la personne concernée et non prévalence de l'intérêt du responsable, disparition du caractère nécessaire des données au regard des finalités… Le § 2 prévoit, au cas où les données, objet de l'opposition, auraient été rendues publiques, le devoir du responsable : « compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, d'informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci ». On retrouve ici la décision de la Cour de justice de Luxembourg, du 13 mai 2014 déjà analysée[53]. Un moteur de recherche qui avait diffusé une donnée obsolète relative à une condamnation ancienne et jugée désormais sans pertinence, a été condamné à « déférencer » les liens vers cette information.

19. Le secret peut s'entendre de la non-révélation de l'auteur d'un message : « Le **droit à l'anonymat sur internet**[54] se déduit de la liberté d'expression et est constitutionnellement garanti par la Loi Fondamentale allemande »[55]. Sans doute, cet anonymat est relatif et n'exclut pas la possibilité pour les instances policières et judiciaires de pouvoir retrouver auprès des serveurs de communication la trace des personnes suspectées

[51] Sur le droit à l'oubli, voy. not. E. Montero et Q. Van Enis, « Les métamorphoses du droit à l'oubli sur le net », *Revue générale de droit civil belge*, n° 5/2016, pp. 243-255.

[52] L'article 18 envisage de manière séparée la limitation des données. Dans ce cas, ce que la personne concernée demande, ce n'est pas l'effacement mais le verrouillage des données qui pourront continuer à être détenues mais non plus utilisées ni *a fortiori* communiquées, sauf consentement exprès de la personne concernée ou dans le cadre d'un recours en justice, sans oublier les droits d'un tiers ou un intérêt public majeur.

[53] Sur cet arrêt, voy., parmi d'autres, E. Defreyne et R. Robert, « L'arrêt "Google Spain" : une clarification de la responsabilité des moteurs de recherche… aux conséquences encore floues », *R.E.D.C.*, 2014, liv. 56, pp. 73-114 ; A. Cassart et J.-F. Henrotte, « Arrêt Google Spain : la révélation d'un droit à l'effacement plutôt que la création d'un droit à l'oubli », *J.L.M.B.*, n° 2014, liv. 25, pp. 1183-1191 ; E. Cruysmans et A. Strowel, « Un droit à l'oubli face aux moteurs de recherche : droit applicable et responsabilité pour le référencement de données « inadéquates, non pertinentes ou excessives », *J.T.*, 2014, liv. 6568, pp. 457-459.

[54] Sur ce droit à l'anonymat y compris en matière de liberté d'expression, lire F. Treguier, « Anonymat et chiffrement, composantes essentielles de la liberté de communication », in *L'Europe des droits de l'homme à l'heure de l'internet* (Q. Van Enis et C. de Terwangne dir.), Bruxelles, Bruylant, 2019, pp. 295-320.

[55] Cour d'appel de Hamm, 3 août 2011.

d'être les auteurs d'infractions graves, dont la liste s'élargit dangereusement d'année en année[56]. À cet égard, le code d'instruction criminelle[57] prévoit certaines prérogatives accordées à de telles autorités de pouvoir pénétrer le système d'information[58] de la personne suspectée et de réclamer la coopération des opérateurs et des prestataires de services de communication au sens le plus large (par exemple : les gestionnaires de réseaux sociaux, les prestataires de services de géolocalisation, etc.) pour procéder à une telle recherche et inspection[59].

Au-delà, la Cour constitutionnelle allemande a consacré l'inviolabilité du « domicile » virtuel que constitue le système d'information propriétaire de la personne concernée, en condamnant l'autorité judiciaire qui dans le cadre d'une enquête relative à des infractions avait utilisé des spywares afin de pénétrer l'ordinateur d'un suspect[60]. Ce jugement rejoint la dis-

---

[56] Directive 2002/58/UE dite directive *e-Privacy*, art. 5. Cette directive une première fois modifiée en 2009 est à nouveau soumise à révision (*cf.* les discussions actuelles au sein de la Commission parlementaire LIBE).

[57] Art. 46 CIC : « § 1er. En recherchant les crimes et les délits, le procureur du Roi peut, par une décision motivée et écrite, procéder ou faire procéder sur la base de toutes données détenues par lui, ou au moyen d'un accès aux fichiers des clients des acteurs visés à l'alinéa 2, premier et deuxième tirets, à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service visé à l'alinéa 2, deuxième tiret, ou bien du moyen de communication électronique utilisé ;

2° l'identification des services visés à l'alinéa 2, deuxième tiret, auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

- de l'opérateur d'un réseau de communications électroniques, et
- de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques ».

[58] La notion est bien plus large que le simple terminal dans la mesure où l'inspection pourra s'étendre à partir du terminal à d'autres lieux de traitement connectés à ce terminal et qui sont laissés à la maîtrise de l'utilisateur du terminal (ainsi, en cas de *télébanking*, les *directories* réservées au client de la banque, le dossier télématique médical tenu à disposition du patient, les services cloud offerts, etc.).

[59] Ainsi, les opérateurs et prestataires de services de communication sont devenus les collaborateurs forcés des autorités judiciaires et policières.

[60] *Bundesverfassungsgerichtshof (BverfGH)*, 27 février 2009. Saisie du recours d'une personne suspectée d'une infraction légère contre les autorités policières qui avaient introduit dans son ordinateur un logiciel espion afin de suivre les activités de ce suspect, la Cour constitutionnelle a condamné, le 27 février 2008, les pratiques policières de recherche on line via des chevaux de Troie. Elle affirme le droit fondamental à la garantie à la sécurité et à l'intégrité de ses systèmes techniques d'informations (« *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme* »). Ainsi, l'intrusion non

position plus large de la directive *e-privacy*[61] qui subordonne au consentement du souscripteur ou de l'utilisateur d'un terminal l'intrusion ou le stockage d'informations dans ce terminal.

À travers l'ensemble de ces prescrits, se dégage la volonté d'affirmer toujours plus le droit des individus à être laissé seuls, c'est-à-dire à la non-transparence. La *Privacy*, entendue comme condition de l'épanouissement de chaque individu ne s'entend pas uniquement de la possibilité de connaître la circulation de son image informationnelle voire à la contrôler mais également de son droit à ne pas se révéler et à rester, ne serait-ce qu'un temps, en dehors de toute connexion numérique à la société (droit de déconnecter son ordinateur, GSM ou GPS ou son tag RFID), ce que nous avons appelé le « droit à la séclusion », à l'opacité et à la solitude[62].

20. Le 25 mai 2017, entrait en vigueur le RGPD[63]. Quelques points sont à signaler sur les développements depuis cette mise en vigueur. En particulier, nombre de déclarations et recommandations ont été depuis émises en matière de systèmes d'intelligence artificielle dont l'utilisation est de plus en plus généralisée tant dans le secteur privé (profilage, robots à finalités diverses) que dans le secteur public (lutte contre la fraude, le terrorisme). On note en particulier la présentation, le 8 avril 2019 d'un code de conduite (*guidelines*) pour un « système d'intelligence artificielle digne de confiance » et d'un *policy document*. La Commission réclame que les systèmes d'IA respectent des valeurs éthiques comme le respect de l'autonomie de la personne, l'explicabilité (*explainability*), la loyauté et la prévention des dommages[64]. Dans le cadre de l'application du RGPD,

---

consentie, dans la puce d'un RFID ou d'un mobile, d'un logiciel pouvant à tout moment révéler notre localisation doit être interdite. On ajoute que l'article 5.3 de l'actuelle directive *e-Privacy* conforte le raisonnement. Cet article prohibe « l'utilisation de capacités de traitement ou de stockage d'informations d'un équipement terminal (par exemple cookies en provenance de tiers ou accès à des images stockées sur un mobile) et la collecte d'informations en provenance de ce terminal ».

[61] Directive 2002/58/UE dite directive *e-Privacy*, art. 5. Cette directive, une première fois modifiée en 2009, est à nouveau soumise à révision (*cf.* les discussions actuelles au sein de la Commission parlementaire LIBE).

[62] A. Rouvroy et Y. Poullet, « The Right to Informational Self-Determination and the value of Self-development : Reassessing the importance of Privacy for Democracy », in S. Gutwirth, Y. Poullet *et al.* (eds), *Reinventing Data Protection*, Springer, 2009, pp. 62 et s.

[63] Le lecteur trouvera un exposé complet sur l'actualité du RGPD dans l'ouvrage collectif du CRIDS : *Le règlement général sur la protection des données (RGPD/GDPR)* (C. de Terwangne et K. Rosier dir.), *op. cit.*, pp. 797 et s.

[64] Disponible à l'adresse : https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-aill s'agit pour la Commission de reprendre les conclusions du High Level Group of experts on AI nommé par la Commission. Sur le rapport de ce groupe, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

le Groupe de l'article 29, depuis dissous et remplacé par l'European Data Protection Board (EDPB) mis en place par le RGPD, a adopté le 18 avril 2018 deux *Guidelines*, dans la matière qui nous occupe, l'un précisément sur la transparence (WP 259) qui exige de la part du responsable du traitement une information dans un « format, concis, transparent, intelligible et facilement accessible, utilisant un langage clair et en termes simples, spécialement pour un enfant » ; l'autre, sur le consentement (WP 260) qui rappelle que le silence ou des cases pré-cochées ne peuvent suffire[65]. Autant de manifestations qui témoignent de l'importance croissante accordée au besoin de transparence du responsable du traitement et de ses traitements y compris son utilisation des systèmes d'intelligence artificielle.

CHAPITRE 3. Les secrets professionnels à l'ère du numérique[66]

21. Les secrets professionnels, ceux du médecin, de l'avocat, du pharmacien mais, également, de toute une série de professions dépositaires des confidences de leurs clients ou des personnes qui sont confiées à leur soin, le secret des sources journalistiques mais également les devoirs de confidentialité consacrés pour certaines professions comme celle de banquier ont la vie dure dans notre société du numérique. Les dialogues singuliers qui les fondent et que le droit entend protéger s'évanouissent au gré des réseaux qu'ils empruntent. Soyons clairs : les technologies de l'information et de la communication multiplient les flux et transforment le dialogue à deux en un dialogue à voix multiples au sein de réseaux toujours plus larges, censés apporter un plus dans la qualité des soins ou des conseils à la personne à l'origine du secret : le patient, le justiciable. Le secret se partage au sein de ces réseaux ; il s'étend à des sous-traitants, sociétés informatiques chargées de stocker ou de traiter des données et dès lors se dilue. On ajoute que les ordres professionnels eux-mêmes, les autorités publiques encouragent les initiatives et favorisent ces échanges au nom tantôt de la diminution des coûts, tantôt de la meilleure qualité

[65] Ces *Guidelines* sont disponibles sur le site de l'EDPB : https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[66] Cette partie synthétise et actualise l'article de l'auteur : « Secret professionnel et les technologies de l'information et de la communication », in *le secret professionnel* (D. KIGANAHE et Y. POULLET eds), in Actes du colloque organisé par l'Association des juristes namurois, 2002, pp. 250 et s.

des soins, tantôt enfin de la sécurité dont ils entourent les communications. Cette circulation permet également un contrôle des prestataires et autorise nos autorités à la prise de mesures d'économie ou de rentabilité du secteur.

Autre cause de ce partage, la technologie oblige à étendre le cercle des détenteurs de secret. Ainsi, les techniciens de laboratoire ou de salles d'opération, les secrétariats administratifs des officines, des hôpitaux, des cabinets d'avocat, les gestionnaires des bases de données tenus dans ces cadres professionnels, tous ont mille raisons d'invoquer leur droit d'accéder aux secrets. Sans doute on peut craindre que cette extension vers des catégories professionnelles nouvelles, non imprégnées de cette culture du secret, ne mette en péril ou en tout cas n'affadisse la rigueur des secrets.

Secret partagé mais également secret déposé : les avantages d'une technologie qui permet l'accès sécurisé à tout moment tout en le restreignant, ajoutera-t-on aux seules personnes autorisées, suggèrent aux patients de déposer leur secret… dans l'attente de la lecture par autrui. Le dialogue n'est plus à l'origine du secret, il suivra peut-être. La volonté de favoriser l'effectivité du service au client justifie la création de vastes répertoires où sont identifiées a priori les relations entre les clients et leurs « confesseurs ». On pense à l'efflorescence des dossiers « santé » déposés sur des serveurs privés ou publics dans le cadre de réseaux télématiques de santé locaux, régionaux[67] voire fédéral ; on songe au répertoire des testaments qui permet à chaque notaire de connaître leur existence préalable et de contacter le confrère *ad hoc*. Dans cette atmosphère de relativisation de

[67] Ainsi, le réseau santé wallon : https://www.reseausantewallon.be ; celui bruxellois : http://brusselshealthnetwork.be.

67*bis*. Sur la plateforme fédérale d'échanges : https://www.ehealth.fgov.be/fr. À propos des risques d'atteinte au secret professionnel médical posé par la plateforme fédérale e-Health, lire l'avis du 10 juin 2010 de l'Académie royale de médecine, Avis concernant l'échange électronique de données relatives à la santé (protection de la vie privée) -Réponses de l'Académie royale de Médecine de Belgique au questionnaire envoyé par la Commission de la Protection de la Vie Privée concernant l'échange électronique de données relatives à la santé : « Les bénéfices apportés au patient et à la collectivité par l'informatisation des services, même si la preuve de ces bénéfices n'a pas encore été réellement apportée à ce jour, risquent de mettre en péril le respect de la vie privée et davantage encore le caractère intime et unique du colloque singulier médecin-patient.

- Le projet e-Health ouvre une brèche dans ce qu'il y a de plus profond et de plus précieux dans la relation médecin-patient : le secret professionnel et la liberté de chacun. Les conséquences à long terme de cette situation peuvent être imprévisibles et incontrôlables.

- L'étanchéité parfaite entre, d'une part, les données personnelles des patients recueillies par les professionnels de la santé dans le cadre des activités de soins, et d'autre part, les données collectives codifiées rendues anonymes et impersonnelles par regroupement de données individuelles collectées à des fins de gestion, d'études ou d'évaluation pour divers organismes et institutions, n'est pas garantie. Cette étanchéité doit être telle qu'il soit

la valeur du secret professionnel, on ne s'étonne pas que ce secret désormais partagé ou déposé soit également objet de vente, comme l'a montré la révélation d'une cession par des hôpitaux de données relatives à leur patient.

22. À propos de ce dernier événement que les journaux ont relayé avec indignation, la contradiction du comportement des hôpitaux avec les exigences de la loi Vie privée ou Protection des données, que nous avons évoquée au chapitre II a été souligné dans la mesure où cette loi limite considérablement la circulation des données en particulier médicales. L'infraction au secret professionnel a été peu mentionnée. D'où la question : la loi Vie privée ne suffit-elle pas à protéger l'intérêt de la personne concernée, en l'occurrence, le patient et ne doit-on pas dès lors rejeter comme un fruit du passé la protection du secret professionnel ? Si, indéniablement, la loi Vie privée s'applique aux détenteurs de secrets professionnels, responsables de traitement et que l'obligation, en particulier de sécurité des traitements, reçoit du fait du secret une interprétation rigoureuse, il n'empêche que notre conviction est inverse : le secret professionnel apporte une protection complémentaire à celle offerte par les lois de protection des données. Les lois de protection des données entendent protéger une partie, le secret professionnel, une relation. Les lois de protection des données soumettent dès lors à la sagacité de la personne concernée, à son consentement, l'utilisation et la transmission de ses données à caractère personnel. À l'inverse, le secret professionnel subordonne la transmission du secret que constitue le fruit du dialogue entre le professionnel et son « client » à une délibération commune, exceptionnellement à un devoir du professionnel de répondre à un intérêt public. Bref, l'application des seules lois de protection des données, à l'exclusion des protections légales accordées au secret, conduit à introduire une « appropriation » du secret par la personne concernée et, donc, pour ce dernier à la possibilité de disposer gratuitement ou contre rémunération du secret vis-à-vis d'autrui, à la limite qu'il s'agisse de son assureur ou de son employeur. À l'inverse, en matière de secret professionnel, le consentement de la personne protégée ne suffit pas à délier le professionnel de son devoir de maintenir le secret : il appartient à ce dernier de s'interroger sur les raisons et la finalité de la demande de son « client » et, le cas échéant, de refuser la transmission des informations couvertes par

impossible, sauf circonstances exceptionnelles et dûment approuvées par l'autorité compétente, de remonter des données collectives aux dossiers des patients, et de stigmatiser ainsi un individu ou un groupe de sujets particuliers ».

le secret au motif que la communication envisagée n'est pas conforme à l'intérêt du « client ».

23. D'autres dangers menacent le secret professionnel. Si le chapitre IV[68] nous permettra d'aborder le danger croissant lié aux lois favorisant ou contraignant la révélation du secret[69] par les dépositaires de secret, notre propos est de revenir un instant sur les nouveaux procédés d'investigation liés à l'utilisation des technologies du numérique, consacrés par le code de procédure criminelle[70] et ses conséquences négatives sur le secret professionnel. Certes, comme le souligne H. Nijs[71] (à propos du secret médical mais le raisonnement vaut bien évidemment pour tous les secrets professionnels), « le législateur n'a jamais eu l'intention d'accorder au cabinet médical une sorte de droit d'asile permettant de soustraire inconditionnellement aux recherches judiciaires aussi bien les documents suspects que les pièces à conviction. Pourtant, l'obligation de garder le secret est impensable sans un droit de garder le secret, qui, à son tour, doit être respecté par la juridiction ». Les possibilités d'accès aux systèmes d'information et aux communications légalisées par l'article 46 du code d'instruction criminelle modifient cet équilibre voulu entre le souci de protection du secret tant professionnel que des communications, d'une part, et les exigences de plus en plus prégnantes de la sécurité publique ou de la lutte contre la criminalité et, d'autre part. En son temps, la Commission belge de protection de la vie privée saisie du projet de loi sur la criminalité informatique[72] qui introduisait les articles 46*bis* et 90*bis* déjà évoqués, avait en vain souligné les risques liés à l'application de ces articles vis-à-vis du secret professionnel : « Par ailleurs, la Commission souhaite attirer l'attention du législateur sur le fait que les textes en projet ne règlent pas la question de savoir dans quelle mesure certains responsables pourront évoquer la règle du secret professionnel

---

[68] *Infra*, n^os^ 23 et s.

[69] L'interdiction de révéler le secret n'existe pas en cas de témoignage en justice ou lorsque la loi explicitement y contraint. Ces obligations de révéler le secret se multiplient dans le cadre des lois INAMI ou de santé publique, de maltraitance des enfants, voire en matière d'assurance terrestre (art. 95 de la loi sur les assurances terrestres. On note que le code de déontologie médicale contient également des invitations à communiquer certains faits pourtant couverts par le secret professionnel. Sur ce mouvement et partageant les réticences de l'auteur, lire également, H. Nijs, *La médecine et le droit*, Kluwer, 1995, pp. 360 et s.

[70] *Supra*, n° 18.

[71] H. Nijs, *La médecine et le droit*, *op. cit.*

[72] Avis de la Commission de protection de la vie privée, n° 33/99 du 13 décembre 1999 relatifs aux projets de loi sur la criminalité informatique. Dans le même sens, l'avis du Conseil national de l'ordre des médecins du 9 janvier 2001 sur les perquisitions dans les cabinets médicaux.

(avocats, journalistes, médecins…). Rien n'est prévu pour que les personnes astreintes au secret professionnel puissent l'invoquer. Les précautions particulières, qu'implique la sauvegarde du secret professionnel face à une perquisition nécessitant l'accès au système informatique, devraient également être réglées. La Commission est d'avis que des mécanismes d'intervention des instances professionnelles devraient légalement être prévus. Ainsi, on pourrait imaginer qu'un membre du Conseil de l'Ordre des médecins ou des avocats soit présent lors de l'intervention des autorités policières ou judiciaires ». On ajoute que le relevé des communications d'un suspect révélera facilement ses liens avec tel avocat et aidera à suivre leur dialogue. C. Forget[73] note à cet égard avec regret que « la loi ne prévoit aucune protection spécifique à l'égard de médecins ou de l'avocat en cas de saisie de données informatiques ou de recherches dans un système informatique[74] ». Par système informatique, il faut entendre tout terminal (un GSM, un objet connecté) mais également tout service assurant la transmission d'information, ainsi What'sApp, Skype, Gmail, Hotmail, Facebook, etc. Au-delà, l'obligation de collaboration des gestionnaires de systèmes d'information avec les autorités policières et judiciaires en matière d'accès aux données et de décryptage des informations oblige, suivant le libellé de l'article 88*quater* du code de procédure criminelle, le responsable du système informatique d'un hôpital ou d'un cabinet notarial ou d'avocats à fournir la liste des clés d'accès et de cryptage, utilisées par les bénéficiaires de ses services. Cette même obligation pourrait peser sur les autorités professionnelles ou les gestionnaires de réseaux mis en place le cas échéant par l'autorité publique (par ex le réseau santé wallon…), tenus de révéler les communications échangées sur les intranets qu'ils gèrent et ce sans que les autorités policières ou judiciaires n'aient à s'adresser aux professionnels destinataires ou émetteurs de ces messages couverts par le secret professionnel[75].

[73] C. Forget, « Méthodes d'enquête pénale et protection des personnes vulnérables », in *Vulnérabilités et droits dans l'environnement numérique* (H. Jacquemin et M. Nihoul coord.), coll. Facultés de droit de Namur, Bruxelles, Larcier, 2018, p. 187.

[74] La remarque est d'autant plus pertinente que la loi du 25 décembre 2016 modifiant certaines dispositions du Code d'instruction criminelle (*M.B.* 17 janvier 2017), c'est tout officier de police judiciaire qui peut effectuer une recherche dans un système informatique. Certaines conditions (la saisie du matériel et l'absence de verrouillage) sont cependant reprises et dans ces cas l'officier devra obtenir l'autorisation du procureur.

[75] Le Conseil d'État avait plaidé pour une exception à propos de tels services, dépositaires de secrets professionnels et ce, comme le notait le Conseil, sous peine de vider l'article 458 du Code pénal de tout sens. L'exposé des motifs de la loi sur la criminalité informatique, sans reprendre l'objection du Conseil et l'exception proposée, semble cependant nuancer le propos de la loi : « En ce qui concerne les personnes tenues par le secret, le but n'est pas de déroger au droit commun en matière de secret professionnel : les personnes tenues par

24. En conclusion, le numérique affadit et affaiblit un secret qu'il pousse de plus en plus à partager et à déposer dans des réseaux dont le fonctionnement est de moins en moins aux mains de la profession. On ajoute que la circulation du secret, son dépôt dans de vastes ensembles certes mieux sécurisés, suscitent des craintes dans la mesure où le numérique accroît les possibilités pour les autorités policières et judiciaires de les pénétrer sans grand souci du respect des impératifs du secret professionnel. Enfin, le numérique, par la facilité d'accès et de communication du dossier, par la transparence de celui-ci, induit une tendance socio-culturelle à plaider pour une appropriation par le client de « son » secret. Cette appropriation subordonne au seul consentement de ce dernier l'utilisation voire la transmission des informations couvertes par le secret. Faut-il se réjouir d'une telle dévalorisation du secret professionnel, sans doute accélérée par les usages du numérique ? À cette question, P. Martens répondait en conclusion d'un colloque tenue en 2002 sur le secret professionnel[76] : « Ce que nous ont appris les débats, c'est que le projet de fraternité universelle ne peut s'accomplir sans l'entretien de liens sélectifs. Une société égalitaire ne suffit pas à produire le bonheur des hommes : elle les laisse dans leur solitude égalitaire, si elle n'est pas aussi une société fiduciaire. Ce n'est pas le droit qui peut aider à bâtir des liens affectifs mais il peut s'attacher à ne pas les détruire. IL est significatif de constater que le secret professionnel se dérobe quand on l'affirme mais qu'il se révèle quand on le nie. : les divulgations obligées par l'article 458 bis du Code pénal pourraient avoir pour conséquences de généraliser la déresponsabilisation, de propager une culture de la délation et de banaliser les repères déontologiques. Or c'est précisément contre ces périls que le secret professionnel nous prémunit parce qu'il évite que la confiance indispensable aux échanges humains ne s'étiole ». Cet appel à la revalorisation de la confiance- et donc du secret- contre la délation et l'affadissement de la déontologie professionnelle constitue précisément le point suivant de notre réflexion.

---

le secret professionnel et agissant dans le cadre du secret professionnel suivent le même régime que si elles étaient amenées à témoigner en justice ; ceci implique un droit et non une obligation de coopérer lorsqu'elles doivent rechercher elles-mêmes des informations spécifiques ». On note que le droit de s'exprimer lors de l'interpellation d'une personne tenue au secret professionnel implique pour cette dernière le droit de se taire.

[76] P. MARTENS, « La société a-t-elle envie du secret ? », in *le secret professionnel* (D. KIGANAHE et Y. POULLET eds), Actes du colloque organisé par l'Association des juristes namurois, 2002, pp. 275 et s.

CHAPITRE 4. La dénonciation érigée en devoir civique[77]

25. Le Parlement européen après avoir très tôt adopté une résolution à propos des « lanceurs d'alerte »[78] [79] reçu, le 12 mars 2019[80], l'aval du « trilogue » sur le texte proposé par la Commission, a finalement approuvé ce 16 avril 2019[81] la directive dite « lanceurs d'alerte ». La directive offre de véritables garanties juridiques et une protection aux personnes qui

[77] Nous tenons particulièrement à remercier Mme A. Lachapelle, doctorante FNRS à l'Université de Namur, pour son aide précieuse dans la rédaction de ce chapitre et renvoyons le lecteur à son intervention publiée dans les actes de ce colloque.

[78] « Cette semaine, les parlementaires européens ont voté un texte qui propose une véritable protection européenne pour les lanceurs d'alerte. IL établit une définition très large pour protéger les lanceurs d'alerte qui va de la fiscalité, la lutte contre la corruption à l'environnement. Ce texte propose de sanctionner toute forme de représailles qui pourrait arriver dans l'environnement professionnel du lanceur d'alerte mais aussi une aide financière et judicaire en cas de procès et enfin la mise en place d'une agence européenne indépendante qui pourrait conseiller les lanceurs. *La députée Virginie Rosière est* l'auteure de ce rapport.

Avec ce texte désormais entre les mains, la Commission pourrait proposer une directive (une loi européenne) pour protéger les lanceurs d'alerte début 2018 ». Café Europe, Samedi 28 octobre 2017, https://www.franceinter.fr/emissions/cafe-europe/cafe-europe-28-octobre-2017. Depuis, la Commission a mis sur la table une « Proposition de directive du 23 avril 2018 relative à la protection des personnes signalant des violations du droit de l'Union (COM(2018) 218 final). Le Conseil, de l'Europe avait dès 2014 émis une recommandation en la matière : Recommandation CM/Rec (2014)7 sur la protection des lanceurs d'alerte, adoptée par le Comité des Ministres du Conseil de l'Europe le 30 avril 2014.

[79] « **Lanceur d'alerte**. Un **lanceur d'alerte** est toute personne, groupe ou institution qui, ayant connaissance d'un danger, un risque ou un scandale, adresse un signal d'alarme et, ce faisant, enclenche un processus de régulation, de controverse ou de mobilisation collective » (Wikipédia).

[80] COM (2018) 218 final. Sur cette proposition de directive, lire A. Lachapelle, « Le lancement d'alerte à l'ère du RGPD », in *Le règlement général sur la protection des données (RGPD/GDPR)* (C. de Terwangne et K. Rosier dir.), coll. Cahiers du CRIDS, n° 44, Bruxelles, Larcier, 2018, pp. 797 et s.

[81] Les eurodéputés ont mis un point final à la directive sur la protection des lanceurs d'alerte le 16 avril, quelques jours après l'arrestation de Julian Assange, le fondateur de Wikileaks. Longtemps jugée infaisable à l'échelle européenne, la protection des lanceurs d'alerte a finalement été adoptée le 16 avril à Strasbourg, lors de la dernière session plénière du Parlement européen avant les élections européennes de mai : « Personne ne pensait que nous arriverions à éditer une règle commune sur la protection des lanceurs d'alerte. […] C'est réellement une victoire », s'est félicitée l'eurodéputée écologiste Eva Joly. L'adoption de la directive – qui ne faisait guère de doute – a largement rassemblé les élus européens qui sont 591 à s'être prononcés en faveur du texte. Seuls 29 eurodéputés ont voté contre et 33 se sont abstenus.

souhaitent s'exprimer lorsqu'elles sont confrontées à des actes illicites ou contraires à l'intérêt général dans le cadre de leurs activités professionnelles. Elle oblige également tous les pays de l'Union européenne à adopter des mesures pour protéger efficacement les lanceurs d'alerte telles que le choix le plus opportun des canaux de signalement, la confidentialité, la protection juridique et les sanctions pour ceux qui tentent d'exercer des représailles contre les « dénonciateurs ». On ajoute que si plusieurs pays ne souhaitaient accorder cette protection qu'après signalement en interne, dans leur structure, entreprise ou organisation, la directive protège le lanceur d'alerte, quel que soit le type de signalement, qu'il soit « en interne », en « externe » ou directement auprès des régulateurs et des autorités compétentes. En outre, les entreprises de plus de 50 employés et les organismes publics seront tenus de mettre en place des canaux et des procédures pour que les lanceurs d'alerte puissent s'y présenter en toute sécurité. Les lanceurs d'alerte ne pourront être poursuivis, ni faire l'objet de représailles mais, en outre, bénéficient d'un *« renversement de la charge de la preuve », c'est à* la personne qui tentera d'exercer des représailles sur un « dénonciateur » d'apporter la preuve que le préjudice infligé n'a pas de rapport avec le signalement. Dernier point, l'obligation pour les États membres de garantir la réparation et l'indemnisation intégrale des dommages subis par les « dénonciateurs », conformément au droit national.

26. Au-delà de ce rapide survol du texte européen, il est sans doute utile d'élargir le propos et de s'interroger sur ce qui devient certes, au travers de nombre de législations mais, au-delà, porté par une volonté de transparence et de moralisation de la vie sociale, un véritable devoir civique[82] : la dénonciation d'infractions ou, en tout cas, de supposées infractions. Au demeurant, écrit A. Lachapelle[83], « il nous faut encore souligner l'impact du principe de transparence sur le renforcement du *whistleblowing* ». Dans ce contexte, la figure du lanceur d'alerte apparaît tout naturellement comme contribuant « au développement d'une plus grande

[82] Comme en attestent deux articles souvent cités : J.-P. Brodeur et F. Jobard, « Conclusion : le pouvoir obscur de la délation », in J.-P. Brodeur et F. Jobard (dir.), *Citoyens et délateurs. La délation peut-elle être civique ?*, Paris, Autrement, 2005, pp. 212-213. S. Brahy, « Dénonciation officielle et dénonciation civique », mercuriale prononcée le 1er septembre 1978 à l'audience solennelle de la cour d'appel de Liège, *Rev. dr. pén.*, 1978, p. 948.

[83] A. Lachapelle, « La dénonciation de faits d'intérêt fiscal : entre *Big Brother* et *Robin Hood* », in *Law, Norms and Freedoms in Cyberspace/Droit, normes et libertés dans le cybermonde : Liber Amicorum Yves Poullet* (C. de Terwangne, E. Degrave, S. Dussolier, R. Queck dir.), Bruxelles, Larcier, 2018, pp. 171-172 ; voy. égal., J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », in *Les lanceurs d'alerte. Quelle protection juridique ? Quelles limites ?* (M. Disant et D. Pollet-Panoussis dir.), Issy-les-Moulineaux, Lextenso, 2017, p. 110.

culture civique de nature à rééquilibrer les relations entre les citoyens et la sphère publique notamment. Il contribue plus généralement à la moralisation des secteurs public et privé ». L'auteure (il s'agit en l'occurrence de Jennifer Marchand) en conclut que le droit d'alerte constitue le « substrat de la société de la transparence ». Notre propos mentionnait déjà dans le même sens les obligations de collaboration des responsables des services informatiques à établir la « vérité judiciaire » (*cf*. chapitre III, *supra*, n° 23).

La technologie du numérique n'est pas étrangère à ce mouvement[84] : les facilités qu'elle offre de transmettre des dossiers voire des dossiers volumineux à l'appui des affirmations du lanceur d'alertes, la possibilité de délivrer des informations anonymement[85], l'accès aisé à des plateformes de diffusion, tout cela contribue à considérer que la dénonciation qui, autrefois, s'opérait difficilement, dans des arrière-cours ou sous le manteau, auprès d'un journaliste dont on espérait qu'il donnerait écho à la nouvelle, est désormais monnaie courante et doit l'être à l'ère où le numérique rend, de manière générale, nos gestes et nos actions transparents et de façon plus particulière, nos comportements dangereux, illégaux voire immoraux.

27. On note la multiplication des régimes de dénonciation qui pèsent sur nombre de catégories professionnelles dont certaines pourtant sont tenues par le secret professionnel ou d'un devoir de confidentialité comme le banquier. On épingle ainsi le nombre de législations qui instaurent un

---

[84] Comme le note W. Vandekerckhove, « European *Whistleblowing* Policies : Tiers or Tears ? », in *A Global Approach to Public Interest Disclosure : What Can We Learn from Existing Whistleblowing Legislation and Research ?* (D.B. Lewis ed.), Cheltenham, Edward Elgar, 2010, chap. 3, p. 17. L'essor des nouvelles technologies de l'information et de la communication a conduit à l'émergence d'une troisième forme de signalement, le signalement public (« *public reporting* »), effectué auprès d'un journaliste, d'un parlementaire, d'une organisation non gouvernementale ou directement auprès du public, via les réseaux sociaux notamment. Sur le lien entre technologies de l'information et de la communication et ampleur du phénomène du « signalement », lire A. Lachapelle, « La protection des lanceurs d'alerte », in *L'Europe des droits de l'homme à l'heure d'Internet* (C. de Terwangne et Q. Van Enis dir.), Bruxelles, Bruylant, 2019, n^os^ 20 et s. *Cf.* égal., sur ce thème, R. De Quenaudon, « Les lanceurs d'alerte », in *Prendre la responsabilité au sérieux* (A. Supiot et M. Delmas-Marty dir.), Paris, P.U.F., 2015, p. 293.

[85] « La plateforme WikiLeaks, créée en 2006, offre un tel anonymat en s'appuyant sur le réseau TOR (le nom dérive de l'acronyme du projet de logiciel d'origine, intitulé « The Onion Router »), le logiciel TAIL (« The Amnesic Incognito Live System ») et la monnaie virtuelle Bitcoin. D'autres plateformes ont été créées depuis lors et se fondent sur la même technologie. On pense au site www.source.eu, le site d'envoi anonyme de documents vers les médias, et à la plateforme « EuLeaks », lancée par les parlementaires européens du groupe Verts/ALE ». A. Lachapelle, « La protection des lanceurs d'alerte », *op. cit.*, n° 21.

devoir de dénonciation, qu'elles soient en matière de terrorisme[86], de fraudes sociale ou fiscale[87], de blanchiment d'argent[88] ou d'abus de marché[89], de corruption[90], d'enfants ou de femmes battues. On souligne que nombre de ces législations visent des personnes tenues au secret professionnel, ainsi les avocats, notaires et travailleurs sociaux ou des personnes tenues d'un devoir de discrétion comme les banquiers. À propos de ces

[86] La loi votée le 4 mai 2017 prévoit une modification du code d'instruction criminelle pour contraindre les travailleurs sociaux, sous peine de sanctions pénales, à communiquer des renseignements personnels dans le cadre d'enquêtes terroristes. Les associations comme le Conseil d'État dénoncent la rupture du lien de confiance entre les travailleurs sociaux et les demandeurs d'aide, de même que la violation du secret professionnel. « (Si le Conseil d'État a peu de remarques à propos de l'obligation des travailleurs sociaux de répondre aux interrogations des autorités policières et judiciaires)… le Conseil d'État se montre en revanche beaucoup plus critique sur l'obligation de dénonciation active. S'ils prennent connaissance d'une ou de plusieurs informations pouvant constituer des indices sérieux de l'existence d'une infraction terroriste, les travailleurs sociaux sont également tenus de les dénoncer. L'avis pointe du doigt le risque d'insécurité juridique. Quelles sont au juste les informations visées ? Est-il question des actes préparatoires, demande notamment le Conseil d'État qui s'interroge sur la notion d'"existence" d'une infraction alors que le délégué du gouvernement a évoqué la "prévention" d'une infraction. Le travailleur social ne pourra pas toujours apprécier aisément l'intention de la personne à propos de laquelle il apprend des informations, fait-il en outre remarquer. "L'obligation générale de communiquer des renseignements, et pas seulement celle liée à une infraction terroriste existante, mais également celle qui tendrait à prévenir ces infractions, sans appliquer la moindre différentiation en fonction de l'infraction, aurait un champ d'application à ce point étendu qu'elle affecterait le secret professionnel dans sa substance, l'obligation de dénonciation n'étant ainsi plus proportionnée, dans certains cas, au but poursuivi", avertit la haute instance d'avis, qui recommande de réexaminer le texte » (Belga, 8 décembre 2016).

[87] En matière sociale, un système de dénonciation au point de contact « pour une concurrence loyale » a été mis sur pied en Belgique (https://www.meldpuntsocialefraude.belgie.be/fr/index.html).

En matière fiscale : reconnaissance de la dénonciation « civique » au travers de questions parlementaires, des jurisprudence et pratique administratives. Le devoir de collaboration des tiers est analysé par certains auteurs comme une obligation spécifique de dénonciation.

[88] Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces, *M.B.*, 6 octobre 2017.

[89] La loi du 31 juillet 2017 modifiant la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, en vue de mettre en œuvre le règlement n° 596/2014 sur les abus de marché et de transposer la directive 2014/54/UE relative aux sanctions pénales applicables aux abus de marché ainsi que la directive d'exécution 2015/2392/UE concernant le signalement des violations, et portant des dispositions diverses, *M.B.*, 11 août 2017.

[90] Loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.*, 4 octobre 2013. *Cf.* égal. les articles 29 et 30 du Code d'instruction criminelle.

derniers, une thèse récente[91] analyse de façon détaillée les divers devoirs de dénonciation du banquier et souligne le dilemme du banquier, tiraillé entre la confiance que lui prodigue son client et son devoir légal sur base de simples soupçons de trahir cette confiance.

Plus inquiétant encore, les dénonciations organisées sans aucune base légale pour des raisons certes louables mais qui risquent de conduire à des calomnies ou à des effets disproportionnés. Ainsi, si la cause de la protection des animaux mérite indéniablement notre appui, faut-il pour autant encourager, par la création d'une plateforme gérée par les pouvoirs publics, la délation entre voisins voire la publication de ces assertions parfois non fondées ?

28. Il est certain que la dénonciation doit être réglementée par la loi même si son principe est incontestable et s'appuie sur la liberté d'expression[92]. Ainsi, dans plusieurs arrêts, la Cour européenne des droits de l'homme juge que la révélation publique d'informations, fussent-elles confidentielles, pouvait tomber sous le coup du droit à la liberté d'expression, consacré à l'article 10 de la Convention européenne des droits de l'homme. On ajoute – le point est important – qu'à cette occasion, la Cour met en balance, d'une part, le droit à la liberté d'expression, et, d'autre part, le devoir de loyauté, de discrétion et de secret auquel les travailleurs, qu'ils relèvent du secteur privé ou public, sont tenus. Pour faire bref, la

[91] D. Goens, *Informatie inwinning bij financieleverrichtingingen op het snijvlak van transparentie en gegevensbeschermong*, Thèse, Universiteit Gent, 2016. L'auteure met bien en évidence les limites au devoir de parler de la banque sur base tant d'un devoir de confidentialité que de la loi de protection des données : « *BRUYNEEL houdt in een betoog voor het verstrengen van de discretieplicht tot een beroepsgeheim in hoofde van de financiële instelling. Dergelijk beroepsgeheim zou enerzijds dergelijke ongewenste doorgiftes van persoonsgegevens aan derden kunnen verhinderen, maar anderzijds dreigt het ook de commerciële exploitatiemogelijkheden van de financiële instelling overmatig te beperken. Dergelijk beroepsgeheim zou in zekere zin zelfs het recht op informationele zelfbeschikking van de betrokkene kunnen beperken daar het toestemmen met bepaalde gegevensverwerkingen niet steeds mogelijk zal zijn. Het voorzien van een bankgeheim zou kunnen leiden tot een te groot paternalisme ten opzichte van de cliënt. Een ander alternatief om de ongewenste doorgifte van persoonsgegevens te verhinderen is om, in geval van toestemming van de cliënt met de doorgifte van persoonsgegevens aan een derde, de cliënt een onmiddellijk economisch voordeel te verstrekken van de doorgifte* ».

[92] La Cour européenne des droits de l'homme (Cour eur. D.H., arrêt *Bargão et Domingos Correia c. Portugal*, 15 novembre 2012, § 35) a étendu, dans son arrêt *Bargão et Domingos Correia*, le droit de dénoncer aux « usagers des services publics dans la mesure où ils ont connaissance ou utilisent les opérations internes du service en cause ». Au-delà de cet arrêt, peut-on justifier non pas la liberté de parler mais l'obligation de parler sur les exceptions de l'alinéa de l'article 10 de la Convention européenne des droits de l'Homme ? Une telle conclusion m'apparaît dangereuse. Ce que l'alinéa vise, ce sont des restrictions à la liberté de parler mais non des justifications d'une obligation positive de prise de parole.

doctrine résume comme suit les principes dégagés par la Cour des droits de l'homme[93], « l'information publiée doit (i) présenter un intérêt public et (ii) être authentique, c'est-à-dire exacte et digne de crédit (iii) la divulgation au public ne doit intervenir qu'en dernier ressort, à savoir si la dénonciation au supérieur hiérarchique ou à l'autorité compétente n'est pas efficace (iv) l'intérêt du public d'obtenir l'information dénoncée doit peser plus lourd que le dommage supporté par l'employeur (v) le dénonciateur doit agir de bonne foi et avec la conviction que l'information était authentique (vi) enfin, la gravité de la sanction encourue par le dénonciateur est prise en considération par le juge »[94].

En d'autres termes, la dénonciation ou le signalement ne peuvent-être « sauvages » sous peine de permettre n'importe quelle vengeance privée. La loi française Sapin II[95] à la suite de la Recommandation (2014)7 du Comité des Ministres du Conseil de l'Europe sur la protection des lanceurs d'alerte[96] établit à cet égard des principes utiles afin de respecter une certaine proportionnalité entre l'intérêt poursuivi par la délation et les risques encourus par les personnes dénoncées : ainsi, la dénonciation ne peut porter que sur des faits graves et en aucune manière sur un secret professionnel. La divulgation suit une procédure par paliers avant de pouvoir être confiée à la presse[97]. C'est en respectant de telles limites qui protègent une autre liberté, à savoir celle d'entreprendre, que le lanceur

---

[93] Sur ces principes, les développements de Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte », in *Le secret*, coll. Recyclage en droit, Limal, Anthemis, 2015, pp. 95-151 ; K. Rosier, « Chapitre III : hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », in *Secret et loyauté dans la relation de travail* (S. Gilson, K. Rosier, A. Roger et S. Palate dir.), Waterloo, Kluwer, 2013, pp. 129-150 ; V. Junod, « La liberté d'expression du *whistleblower*. Cour européenne des droits de l'homme (Grande Chambre), Guja c. Moldova, 12 février 2008 », *Rev. trim. dr. h.*, n° 2009/77, pp. 227-260.

[94] A. Lachapelle, « La protection des lanceurs d'alerte », *op. cit.*

[95] Loi Sapin-II du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique dite Sapin II – articles 6 à 16. Voy. aussi la loi dite Défenseur-des-droits du 9 décembre 2016 relative à la compétence du Défenseur des droits pour la protection des lanceurs d'alerte qui modifie l'article 4 de la loi du 29 mars 2011 relative au Défenseur des droits.

[96] Recommandation du 30 avril 2014 adoptée par le comité des ministres lors de leur 198e réunion.

[97] Le lanceur d'alerte doit procéder dans cet ordre, à défaut de le respecter sa bonne foi et sa responsabilité civile et pénale peuvent être mises en cause devant un tribunal (art. 8 de la loi Sapin II) :

– en premier lieu, le signalement de l'alerte doit être porté à la connaissance de son supérieur hiérarchique, direct ou indirect, ou de son employeur ou d'un référent désigné par l'employeur.

Le destinataire de l'alerte doit alors vérifier, dans un délai raisonnable (la loi ne le fixe pas), la recevabilité du signalement.

d'alerte, travailleur, bénéficiera lui-même de la protection que lui accorde la réglementation et évitera les représailles faciles dues à son statut. Cette protection notamment pour un travailleur peut couvrir une indemnité pour le licenciement encouru suite à la révélation[98]. La loi française dite « Sapin II » va même jusqu'à créer un fonds pour permettre la protection voire la rémunération financière des lanceurs d'alerte[99]. C'est dire l'appui donné par les autorités publiques à ce mouvement civique de lutte contre les « criminels » sans doute la transparence y gagne et le fonctionnement démocratique de nos sociétés, également. On insistera cependant sur la nécessité de balises, d'une protection procédurale des droits de la défense et sur l'insécurité des journalistes confrontés à une avalanche de signalements souvent fantaisistes, inexacts voire calomnieux sans que ces derniers aient toujours les moyens de la vérification[100]. On souligne la dualité d'approche de la légitimité du lanceur d'alerte est mise en évidence de manière heureuse. D'une part, le lanceur apparaît à la fois comme le héros de la liberté d'expression et donc de la démocratie (approche du Conseil de l'Europe). À ce titre, il a le devoir de parler, sans doute en ayant pris certaines précautions, et toutes représailles à son égard méritent, au regard de l'article 10 de la C.E.D.H., d'être sanctionnées (arrêts *Guja*). D'autre part, il peut être considéré comme l'auxiliaire de l'autorité dans la poursuite d'une mise en œuvre effective de sa politique, en particulier fiscale, économique voire de protection des données. Cette seconde attitude

– en second lieu, à défaut de vérification, dans le délai raisonnable, par le destinataire du signalement, le lanceur d'alerte peut saisir l'autorité judiciaire, administrative ou son ordre professionnel, également le Défenseur des droits.

Il peut toutefois saisir directement ces autorités si le signalement concerne un danger grave et imminent ou présente un risque de dommage irréversible… et rendre public ce danger ou ce risque.

– en troisième lieu, possibilité de rendre public le signalement notamment en alertant la presse, si l'autorité destinataire ne réagit pas dans un délai de trois mois après la réception du signalement.

[98] En ce qui concerne les fonctionnaires, voy. la Proposition de loi modifiant la loi du 22 mars 1995 instaurant des médiateurs fédéraux, afin d'assurer une protection légale aux fonctionnaires qui dénoncent des irrégularités, 4 octobre 2010, *Doc. parl.*, Sén., sess. extr. 2010, n° 5-217/1, p. 1.

[99] Selon la Convention des Nations unies contre la corruption, dite « Convention de Mérida » (en anglais, connue sous l'intitulé « UNCAC »), adoptée par l'Assemblée générale par la Résolution n° 58/4 du 31 octobre 2003 et en vigueur depuis le 14 décembre 2005 : « Chaque État Partie envisage d'incorporer dans son système juridique interne des mesures appropriées pour assurer la protection contre tout traitement injustifié de toute personne qui signale aux autorités compétentes, de bonne foi et sur la base de soupçons raisonnables, tous faits concernant les infractions établies conformément à la présente Convention ».

[100] À cet égard, on ne peut que féliciter les journalistes d'avoir, suivant leur Code de déontologie, mis en lumière des affaires comme les *Panama Papers*, le *Luxleak*, etc.

transparaît dans certains textes européens et justifie la « rétribution » des « délateurs ».

Si la liberté d'expression permet de justifier le lancement d'alerte mais également certaines limites (ainsi, la nécessité d'une conviction raisonnable de la véracité de l'information, l'intérêt public à la connaissance de celle-ci) et la protection de la révélation lorsqu'elle est le fait d'un journaliste ou rapportée par ce dernier, la protection de la vie privée ajoute d'autres éléments à la protection du lanceur d'alerte (secret des correspondances, droit au suivi du signalement…) mais également entend protéger les personnes qui, le cas échéant, se voient dénoncées. À cet égard, on s'interroge, au-delà du devoir de confidentialité du signalement et de son auteur, sur l'existence d'un « droit au chiffrement et à l'anonymat » du lanceur d'alerte, non consacré à l'heure actuelle. Enfin, on s'inquiétera au moment où l'Europe s'apprête à reconnaître l'apport des lanceurs d'alerte et à les protéger, de voir cette même Europe consacrer les secrets d'affaires et dès lors protéger cette fois les intérêts des entreprises au détriment de la transparence voulue. Nous reviendrons sur ce point dans la section que nous abordons maintenant.

CHAPITRE 5. Transparence et accès aux savoirs

29. « La capacité de chacun d'accéder à l'information aux idées et au savoir et d'y contribuer est essentielle dans une société de l'information inclusive », proclamait la Déclaration de principes du Sommet mondial de la société de l'information de 2003[101]. Sans doute, ce principe exprime un vœu cher aux créateurs de l'Internet, à savoir en faire un outil qui permette à chaque citoyen du monde de pouvoir acquérir les connaissances et s'exprimer dans une société devenue de l'information ; est-il pour autant devenu réalité ? Cette dernière section examine deux tendances contradictoires de nos législations et de nos pratiques. La première, à la faveur des possibilités offertes par le numérique et du fait que l'Internet soit devenu une ressource publique mondiale, au même titre que l'eau, plaide pour une diffusion maximale des savoirs. La seconde, au contraire, au nom d'intérêts économiques certes dignes de protection, entend réserver le savoir ou en tout cas en permettre l'appropriation… notamment grâce à la technologie. Bref, entre transparence et secret, le droit hésite.

[101] Il s'agit du principe n° 24. Le SMSI a été organisé par les Nations unies sous l'impulsion de son secrétaire général et se veut une sorte de Constitution de l'Internet global.

Notre propos entend en effet montrer que le droit de la propriété intellectuelle qui permet l'appropriation du savoir a étendu son champ d'application à la protection de l'information. Au-delà, dans le cadre en particulier de la directive européenne récente sur la protection des secrets d'affaires et des informations commerciales non divulguées, le droit européen renforce la protection des secrets d'entreprise et ce même droit consacre la légalité des mesures techniques de protection des œuvres, au-delà des équilibres traditionnels établis par les législateurs de la propriété intellectuelle. Parcourons ces trois points avant d'analyser la première tendance plus favorable à la transparence.

30. Sans pouvoir détailler chaque affirmation, ce qui nous conduirait à tout un ouvrage[102], nous affirmons que le droit de la propriété intellectuelle s'est mis au service de la technologie du numérique. La protection par le droit d'auteur des logiciels a été décidée par les entreprises du secteur afin de pouvoir bénéficier d'une protection juridique reconnue universellement : cette protection n'a cessé de heurter la doctrine de nos pays. Cette dernière avait du mal à comprendre en dehors de quel cas comment le logiciel, moyen technique d'accomplir certaines tâches et non œuvre, pouvait bénéficier d'une protection alors même que le contenu du logiciel, le programme source n'était pas communiqué. Les auteurs rappellent que la protection par le droit d'auteur a pour objectif de nourrir l'« espace public » de la connaissance et des idées et non de réserver l'usage de la soi-disant œuvre aux seuls licenciés[103]. Au-delà nombre de critiques ont été adressées vis-à-vis de l'extension considérable et croissante donnée à la protection par le brevet des logiciels. Enfin, la protection *sui generis* par le droit européen des bases de données consacre une dérive vers la protection *a priori* de l'investissement d'une entreprise, investissement qui, jusque-là, était protégé en grande partie par le droit de la concurrence déloyale.

---

[102] *Cf.* toutefois sur ces arguments et les références, l'étude réalisée pour l'UNESCO ; S. Dusollier, Y. Poullet et M. Buydens, « Droit d'auteur et accès à l'information dans l'environnement numérique », International Congress, INFOETHICS 2000, Ethical, Legal and Societal Challenges of Cyberspace, Paris 2000, publié in *Bulletin du droit d'auteur*, XXXIV, 4, oct. 2000, pp. 4 à 36.

[103] « Toutefois, ce renforcement du droit d'auteur risque de provoquer une rupture sans précédent de l'équilibre inhérent à tout système de propriété intellectuelle. Le droit d'auteur repose en effet sur un équilibre, une balance d'intérêts entre la protection de la création et des auteurs et la garantie de l'intérêt public et des libertés fondamentale. Cet équilibre résulte notamment d'un des fondements essentiels du droit d'auteur qui est de promouvoir le progrès des sciences et des arts et la diffusion de la culture » (S. Dusollier, Y. Poullet et M. Buydens, « Droit d'auteur et accès à l'information dans l'environnement numérique », *op. cit.*, p. 6).

31. La récente protection des secrets d'affaires et des informations commerciales non divulguées offertes par la directive 2016/943[104] consacre une protection *sui generis* du secret d'affaires[105] (secrets de fabrication, liste de contacts, base de données de clientèle, procédure d'approche du marché, plan stratégique…), jusque-là protégé pénalement dans le cadre de divulgation par les employés mais surtout par le droit de la concurrence déloyale qui imposait de lourds devoirs de preuve (dommage subi, faute de la personne à l'origine du comportement…)[106]. Désormais, la protection du secret permet à son détenteur de prendre, à l'instar des mesures existantes en matière de propriété intellectuelle, outre des mesures provisoires et conservatoires de manière à prévenir toute augmentation du dommage et sa future réparation, des mesures au fond comme la cessation de la commercialisation des produits en infraction ou leur acquisition. Surtout, il ouvre la voie à la réparation du préjudice calculé selon le principe indemnitaire, voire, le cas échéant la publication de la décision judiciaire.

---

[104] Directive 2016/943/UE du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites, *J.O.U.E.*, 15 juin 2016, L. 157/1 à L. 157/18 « Aux fins de la directive, on entend par « secret d'affaires », des informations qui répondent à toutes les conditions suivantes : a) elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles ; b) elles ont une valeur commerciale parce qu'elles sont secrètes ; c) elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes » (art. 2).

[105] L'article 2.1.de la directive définit les secrets d'affaires comme les informations tenues secrètes, c'est-à-dire inconnues en général des personnes appartenant aux milieux concernés, qui ont une valeur commerciale parce que secrètes et qui font l'objet de protections pour être maintenu secrètes. A. Strowel (« Les données : des ressources en quête de propriété, Regards sur quelques développements récents en droit européen », in *Law, Norms and Freedoms in Cyberspace/Droit, normes et libertés dans le cybermonde : Liber Amicorum Yves Poullet* (C. DE TERWANGNE, E. DEGRAVE, S. DUSSOLIER, R. QUECK dir.), Bruxelles, Larcier, 2018, pp. 264 et s.) parle de « quasi-propriété ».

[106] Sur ce point, les réflexions de V. CASSIERS et A. STROWEL, « La directive du 8 juin 2016 sur la protection des secrets d'affaires », in *Le secret*, coll. Recyclage en droit, vol. 4, Limal, Anthemis, 2017, pp. 40 et s. Les auteurs, à la suite d'ailleurs des considérants de la directive, rejettent la qualification de droit de la propriété intellectuelle qu'assure la protection du secret des affaires. Ils notent toutefois que « l'inclusion des "biens en infraction" constitue une objectivation de la protection… et que cette extension de la protection tend donc à créer une quasi-propriété intellectuelle ou un droit *sui generis*, en tout cas un régime qui ne se limite pas à sanctionner une conduite mais s'étend aux produits dérivés ». Le lecteur se référera à ce texte pour l'analyse des points évoqués ci-après.

Cette protection du secret d'affaires a été fortement critiquée par la presse[107]. La directive fait la part trop belle aux intérêts de l'entreprise à l'opacité et négligeait l'intérêt public à la transparence. Ainsi dans quelle mesure, la référence à l'existence d'un secret d'affaires ne contribuerait-elle pas à soustraire l'entreprise à ses devoirs de transparence envers l'État ? Dans quelle mesure, ne constituerait-elle pas un argument dirimant contre toute révélation par un lanceur d'alerte dont la section précédente chantait les mérites de l'intervention ? Cette tension entre ces intérêts et la nécessité de trouver un équilibre est cependant bien présente dans le texte de la directive et ses considérants même si l'interprétation des nuances ainsi apportées ne rassure pas les tenants de la transparence. Il est intéressant de noter que les parlementaires européens ont explicitement réclamé que la directive sur les lanceurs d'alerte soit adoptée comme un contrepoids à celle sur le secret d'affaires. Notre crainte de voir la directive « Secret des affaires » rendre difficile le lancement d'alerte est donc, à la lecture de la directive qui consacre la protection du lanceur d'alerte partiellement levée dans la mesure où ce sera à un tiers et en définitive au juge à trancher sur la réalité du secret invoqué :

> « L'article 2.1, c) et d) de la directive effleure, notent Cassiers et Strowel[108], la question de l'équilibre entre protection des secrets et promotion de la transparence dans l'accès aux documents. Où le droit privé (à contrôler une information confidentielle) entre directement en conflit avec un intérêt public (à faire circuler une information utile au public) ». Ainsi, l'entreprise ne pourrait, au nom du secret d'affaires, s'opposer aux demandes de renseignements de l'administration ni, secondement et dans la foulée, aux communications que les autorités publiques pourraient opérer dans le cadre de l'application des lois sur la transparence administrative (supra sur cette transparence, Section I). Cette seconde conclusion doit cependant être fortement nuancée au vu du libellé du règlement dit « transparence » n° 1049/2001, qui définit les exigences de publicité pour les institutions européennes et sert de modèle aux législations nationales d'accès aux documents administratifs. En effet, l'article 4.2 de cette directive prévoit que les secrets commerciaux et les intérêts commerciaux d'une personne physique ou morale constituent des objections à la divulgation par l'autorité publique des informations

[107] « À la faveur de sa couverture médiatique, il nous faut encore brièvement évoquer la directive « secret d'affaires ». L'adoption de cette directive, à peine deux mois après que n'éclate le scandale des *Panama Papers*, fut accueillie avec hostilité par la presse et l'opinion publique » (A. LACHAPELLE, « La protection des lanceurs d'alerte », *op. cit.*, n° 32).

[108] V. CASSIERS et A. STROWEL, « La directive du 8 juin 2016 sur la protection des secrets d'affaires », *op. cit.*, pp. 68 et s.

relatives à ces secrets ou intérêts sauf à démontrer l'intérêt public supérieur à cette divulgation. Bref, il est certain que les entreprises se prévaudront de la reconnaissance légale du secret d'affaires pour s'opposer à la transparence administrative.

L'article 5 de la directive est plus obscur encore. Il contient diverses exceptions à la protection du secret d'affaires. La liberté d'expression semble ne viser que les journalistes dont il serait sinon à craindre que la protection du secret d'affaires n'entrave la liberté d'informer ; la deuxième exception concerne les lanceurs d'alerte, dans la mesure où elle concerne une atteinte au secret « pour révéler une faute, un acte répréhensible ou une activité illégale, à condition que le défendeur ait agi dans le but de protéger l'intérêt public général… ». La formulation laisse entendre que c'est donc au lanceur d'alerte de prouver que sa révélation reprend l'ensemble des conditions du texte ou en tout qu'il y ait cru. La dernière exception englobe les deux premières. Il s'agit d'exonérer de toute responsabilité l'auteur de l'atteinte lorsque celle-ci a été commise « aux fins de la protection d'un intérêt légitime », c'est-à-dire notamment « les droits et libertés fondamentaux, l'intérêt public ; tels que la sécurité publique, la protection des consommateurs, la santé publique, la protection de l'environnement… et la mobilité des travailleurs ». Sans doute, l'exception, certes décrite largement mais comme toute exception à interpréter *in casu* restrictivement, laissera aux juges le soin de pondérer les libertés et intérêts en présence. Lors de ce travail, se poseront aux juges des questions telles que de savoir si la rémunération du délateur n'exclut pas *a priori* le bénéfice de l'exception ou si les *Ethic Hackers* ne se verront pas reprocher leurs intrusions illégales dans des secrets protégés. L'importance des faits dénoncés et la gravité de leur illégalité compenseront-elles le caractère illégal des moyens de mise à jour de cette infraction[109] ?

32. Au-delà de cette extension des « biens » en particulier numériques protégés par le droit ou le « quasi droit » de la propriété intellectuelle, nous souhaitons évoquer un dernier point. L'article 6 de la directive 2001/29 de l'Union européenne sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information énonce : « Les États membres prévoient une protection juridique appropriée contre le contournement de toute mesure technique efficace… ». En d'autres termes, le droit consacre le droit des titulaires de propriété intellectuelle

[109] Sur cette question délicate, nous renvoyons le lecteur aux décisions et écrits suivants : O. Leroux et Y. Poullet, « En marge de l'affaire Gaia : de la recevabilité de la preuve pénale et du respect de la vie privée », *R.G.D.C.*, 2003, liv. 3, p. 167, n° 8 ; Cass., 19 janvier 2016, R.G. n° P. 15.0768.N, p. 4, n° 5 ; C. Buysse, « Dénonciation irrégulière d'un délit par le fisc et doctrine Antigone », *Fiscologue*, 19 février 2016, n° 1464, p. 12.

à utiliser la technologie pour protéger leurs œuvres et protège cette technologie contre tout contournement. On connaît les différentes techniques proposées aux titulaires de droit et surtout à leurs ayants droit : systèmes anti copie, *Digital Rights Management Systems (DRMS), watermarking*, etc. Si ces systèmes poursuivent sans doute un but légitime, à savoir garantir l'effectivité des droits patrimoniaux de leurs détenteurs, on reprochera à certaines de ces mesures leur « sur-effectivité ». Ainsi a été dénoncé le fait que des logiciels anti-copie condamnaient l'utilisateur légitime d'un DVD à ne l'utiliser que sur un appareil de lecture déterminé. On souligne que des logiciels de *watermarking* signent chaque élément de l'œuvre et donc détectent toute copie même d'un élément infime de l'œuvre et cela au-delà de la protection offerte par le droit d'auteur[110]. On dénonce la difficulté de faire valoir au regard d'une technologie aveugle les exceptions prévues par les législations du droit d'auteur, qu'il s'agisse des exceptions de parodie, liées à des utilisations pédagogiques ou de recherche, etc. Enfin, on constate que les systèmes technologiques mis en place aboutissent à un renversement de la charge de la preuve. C'est à celui qui dénie la qualité d'œuvre de l'information ou du document protégé ou qui affirme son droit à l'utiliser nonobstant la protection technique, à démontrer le bien-fondé de sa prétention. Pour ce faire et afin d'en contester le fonctionnement ou la légitimité, encore faudrait-il que le prétendant à l'utilisation puisse exiger la transparence de cette mesure technique.

33. Toutes ces réflexions conduisent à une affirmation : le droit, en particulier de la propriété intellectuelle, protège le secret des œuvres numériques et soumet leur accès aux conditions de ceux qui bénéficient de sa protection. Il est piquant de constater que dans le même temps, le même droit de la propriété intellectuelle peut contribuer à la transparence et à la diffusion de l'œuvre ? Comme le note S. Dusollier, le droit de la propriété intellectuelle est ambigu. Il peut être utilisé tant dans une perspective exclusive comme nous l'avons montré que dans une perspective inclusive : c'est le sens de tous les mouvements *OPEN*[111]*, qu'il s'agisse de*

[110] Sur les mesures techniques et les questions posées par ces mesures aux droits d'auteur, lire, S. Dusollier, *Droit d'auteur et protection des œuvres dans l'univers numérique*, 2e éd., Bruxelles, Larcier, 2007. E. Becker *et al.* (eds), *Digital Rights Management – Technological, Economic, Legal and Political Aspects*, Berlin, Springer-Verlag, 2003.

[111] Favorisés par la doctrine des *Commons* lancée par L. Lessig aux États Unis, *Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, New York, The Penguin Press, 2004. Qu'il soit clair que l'ouverture à l'utilisation et à la transformation de l'œuvre peut ne pas être gratuite mais qu'elle est ouverte à tous et sans autres conditions que le paiement d'une rémunération de l'auteur ou de l'ayant droit et le respect des droits non patrimoniaux.

l'open data, de l'open source ou de l'open document[112] et contribuer ainsi à la création d'un domaine public informationnel[113]. Ces mouvements, pour certains du moins, s'appuient sur une affirmation forte des droits moraux de l'auteur qui renonce à exercer son droit à contrôler l'utilisation voire le développement de l'œuvre mais entend continuer à se prévaloir de son droit à la paternité et au respect de la destination de l'œuvre. Si l'ambivalence du droit d'auteur au regard du choix entre transparence et secret (ou plutôt appropriation du savoir) est bien réelle, il faut cependant constater que, dans les faits, les titulaires des droits d'auteur, à la faveur du droit et de son alliance avec la technologie, penchent décidément vers la restriction de l'accès au savoir au mépris parfois des équilibres souhaités par le droit de la propriété intellectuelle.

34. Ce dernier point nous invite à analyser le quatrième thème évoqué. Le renforcement des droits d'auteur et droits sui generis de tous poils. La directive dite *Copyright in the Digital Single Market* a été approuvée le 26 mars par le Parlement européen après multiples débats et suite à un trilogue à grand suspense[114]. Elle contient notamment l'établissement

[112] Dès 2003, S. Dusollier l'affirmait : « *Copyleft, open source, and other forms of freely available art have at times been announced as the death of copyright. Short of resorting to such extremes, however, one may question the major transformations that this alternative legal model of creation poses to copyright. This paper aims principally to consider authorship in the open source movement. Its hypothesis is that the copyleft licenses espouses and put in practice the new form of authorship that was announced by Foucault in his seminal paper 'What is an author'. The author is not anymore the unique source of meaning but is a founder of discursivity. As the initiator of an open discourse, of an ever-evolving work, the author of an element of a collective creation in copyleft finds her particular contribution diluted by the whole of successive contributions. The "work" in the copyleft regime is software in constant (re)-formation ; it is the production of meaning from different convergent or successive artistic practices. This exercise of copyright in open access licenses is a first attempt to experiment authorship in a way closer to distributive and contemporary artistic practices, and not in the more rigid meaning conferred by copyright to that notion* » (S. Dusollier, « Open Source and Copyleft : Authorship Reconsidered ? », *Columbia Journal of Law & Arts*, 2003, vol. 26, pp. 281-296). De manière plus tranchée encore du même auteur, « L'évolution des figures de la création à l'ère du numérique », in *Law, Norms and Freedoms in Cyberspace/Droit, normes et libertés dans le cybermonde : Liber Amicorum Yves Poullet* (C. de Terwangne, E. Degrave, S. Dussolier, R. Queck dir.), Bruxelles, Larcier, 2018, pp. 371 et s.

[113] En ce sens, l'article de S. Dusollier et V.-L. Benabou, « Draw me a public domain », in P. Torremans (ed.), *Copyright Law : A Handbook of Contemporary Research*, Edgar Elgar, 2007, pp. 161-184. *Cf.* également le plaidoyer de S. Dusollier, « Pour un régime positif du domaine public » article publié sur la toile (mars 2015) à l'adresse suivante : http://romaine-lubrique.org/pour-regime-positif-domaine-public-severine-dusollier.

[114] Directive 2019/790/UE du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE, publiée in *J.O.U.E.*, L 130/92, 17 mai 2019.

d'un nouveau droit voisin sur les publications de presse (art. 15) et la refonte du régime de responsabilité de certains intermédiaires techniques en cas de violation du droit d'auteur par leurs utilisateurs (art. 17[115]). Que dire si ce n'est, à propos du premier point, que les entreprises de presse pourront désormais négocier une rémunération pour les articles repris par les plateformes d'information ou les services de presse d'une certaine ampleur. Sans doute, appréciera-t-on que ceux qui contribuent à la transparence de l'information puissent ainsi retirer une juste rémunération de leur apport à la société même si on peut craindre que cette victoire soit « à la Pyrrhus », lorsqu'il s'agira de négocier avec des géants de l'information et avec la crainte d'un boycott de ceux qui n'accepteront pas les conditions de ces derniers. En ce qui concerne le second point, l'article 17

[115] *Cf.* l'article 17.4. 5 et 6. « Si aucune autorisation n'est accordée, les fournisseurs de services de partage de contenus en ligne sont responsables des actes non autorisés de communication au public, y compris la mise à la disposition du public, d'œuvres protégées par le droit d'auteur et d'autres objets protégés, à moins qu'ils ne démontrent que :

a) ils ont fourni leurs meilleurs efforts pour obtenir une autorisation ; et
b) ils ont fourni leurs meilleurs efforts, conformément aux normes élevées du secteur en matière de diligence professionnelle, pour garantir l'indisponibilité d'œuvres et autres objets protégés spécifiques pour lesquels les titulaires de droits ont fourni aux fournisseurs de services les informations pertinentes et nécessaires ; et en tout état de cause
c) ils ont agi promptement, dès réception d'une notification suffisamment motivée de la part des titulaires de droits, pour bloquer l'accès aux œuvres et autres objets protégés faisant l'objet de la notification ou pour les retirer de leurs sites internet, et ont fourni leurs meilleurs efforts pour empêcher qu'ils soient téléversés dans le futur, conformément au point b) ».

« 5. Pour déterminer si le fournisseur de services a respecté les obligations qui lui incombent en vertu du paragraphe 4, et à la lumière du principe de proportionnalité, les éléments suivants sont, entre autres, pris en considération :

a) le type, l'audience et la taille du service, ainsi que le type d'œuvres ou autres objets protégés téléversés par les utilisateurs du service ; et
b) la disponibilité de moyens adaptés et efficaces et leur coût pour les fournisseurs de services ».

« 6. Les États membres prévoient que, à l'égard de nouveaux fournisseurs de services de partage de contenus en ligne dont les services ont été mis à la disposition du public dans l'Union depuis moins de trois ans et qui ont un chiffre d'affaires annuel inférieur à 10 millions d'euros calculés conformément à la recommandation 2003/361/CE de la Commission, les conditions au titre du régime de responsabilité énoncé au paragraphe 4 sont limitées au respect du paragraphe 4, point a), et au fait d'agir promptement, lorsqu'ils reçoivent une notification suffisamment motivée, pour bloquer l'accès aux œuvres ou autres objets protégés faisant l'objet de la notification ou pour les retirer de leurs sites internet.

Lorsque le nombre moyen de visiteurs uniques par mois de tels fournisseurs de services dépasse les 5 millions, calculé sur la base de l'année civile précédente, ils sont également tenus de démontrer qu'ils ont fourni leurs meilleurs efforts pour éviter d'autres téléversements des œuvres et autres objets protégés faisant l'objet de la notification pour lesquels les titulaires de droits ont fourni les informations pertinentes et nécessaires ».

engendre de sérieuses craintes de la part de ceux qui défendent la cause des libertés[116].

Cette même crainte vis-à-vis du contrôle par les pouvoirs privés s'exprime également en ce qui concerne la lutte contre les *Fake News*. La Commission européenne [117] a, en synergie avec les principales plateformes (Facebook, Twitter, Google, Mozilla, Association des entreprises de publicité en ligne, Microsoft…) adopté en septembre 2018 un « Code de bonnes pratiques contre la désinformation » qui recommande notamment la prise de mesures de vérification (*Fastchecking*, nomination d'un organe de médiation indépendant…) de la qualité des messages, en particulier politiques, qui circulent sur la toile à travers leurs plateformes[118].

---

[116] En particulier EDRI et, en particulier, les articles suivants : Filters Incorporated (19.04.2019) : https://edri.org/filters-inc/. ; Censorship machine takes over internet (26.03.2019) : https://edri.org/censorship-machine-takes-over-eu-internet/ ; Copyright reform : Document pool : https://edri.org/copyright-reform-document-pool/

[117] Code européen de pratique sur la désinformation, disponible sur le site : https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation. « *Representatives of online platforms, leading social networks, advertisers and advertising industry agreed on a self-regulatory Code of Practice to address the spread of online disinformation and fake news. This is the first time worldwide that industry agrees, on a voluntary basis, to self-regulatory standards to fight disinformation. The Code aims at achieving the objectives set out by the Commission's Communication presented in April 2018 by setting a wide range of commitments, from transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation. The Code includes an annex identifying best practices that signatories will apply to implement the Code's commitments. The Commission has also published the opinion of the Sounding board of the Multi-stakeholder forum on the Code of Practice.*

The Code of Practice was signed by the online platforms Facebook, Google and Twitter, Mozilla, as well as by advertisers and advertising industry in October 2018 and signatories presented their roadmaps to implement the Code. In May 2019, Microsoft subscribed to the Code of Practice and also presented its roadmap. Online platforms and trade associations representing the advertising sector have submitted a baseline report in January 2019 setting out the state of play of the measures taken to comply with their commitments under the Code of Practice on Disinformation..Between January and May 2019, the European Commission carried out a targeted monitoring of the implementation of the commitments by Facebook, Google and Twitter with particular pertinence to the integrity of the European Parliament elections. In particular, the Commission asked the three platforms signatory to the Code of Practice to report on a monthly basis on their actions undertaken to improve the scrutiny of ad placements, ensure transparency of political and issue-based advertising and to tackle fake accounts and malicious use of bots. The Commission published the reports received for the five months together with its own assessment ».

[118] On note en particulier le point II D du *Code of Practice* :

« *The Signatories of this Code recognise the importance of diluting the visibility of Disinformation by improving the findability of trustworthy content and consider that users should be empowered with tools enabling a customized and interactive online experience so as to facilitate content discovery and access to different news sources representing alternative viewpoints, and should be provided with easily-accessible tools to report Disinformation, as referred to in the Communication.*

Le 29 janvier de cette année, la Commission publia le premier rapport sur la mise en œuvre de ce Code.

Le texte nouveau, qui modifie sur certains points la directive de 2001, intitulé « Le droit d'auteur dans le marché unique numérique »[119], est intéressant dans la mesure où, premièrement, il accroît le recours aux mesures technologiques, réclamant indirectement aux plateformes de mises en ligne de prévoir des systèmes d'intelligence artificielle, capables de détecter toute copie ; secondement, dans le même temps, le texte demande que soient respectées dans la mise en place de ces systèmes de détection et de blocage, les exceptions prévues par le droit d'auteur. Détaillons ces deux points. Le texte renforce la légitimité de la délégation aux mesures technologiques en particulier même si elles ne sont pas nommées, celles recourant à l'intelligence artificielle. L'article 17 de cette directive impose en effet aux 'fournisseurs de services de partage de contenus en ligne' (en d'autres termes les plateformes de communication et d'informations), selon les termes du considérant n° 66, « de fournir leurs meilleurs efforts, conformément aux normes élevées du secteur en matière de diligence professionnelle, pour éviter que des œuvres et autres objets protégés non autorisés, tels qu'ils sont identifiés par les titulaires de droits concernés, ne soient disponibles sur leurs services. À cette fin, les titulaires de droits devraient fournir les informations pertinentes et nécessaires aux fournisseurs de services en tenant compte, entre autres facteurs, de la taille des titulaires de droits et de leurs types d'œuvres et autres objets protégés ». Ce devoir de prendre des mesures ne vise pas nécessairement des mesures

---

- Relevant Signatories should invest in technological means to prioritize relevant, authentic, and authoritative information where appropriate in search, feeds, or other automatically ranked distribution channels.

- The Signatories of this Code recognize that transparency should be ensured with a view to enabling users to understand why they have been targeted by a given political or issue-based advertisement.

- Such transparency should reflect the importance of facilitating the assessment of content through indicators of the trustworthiness of content sources, media ownership and verified identity. These indicators should be based on objective criteria and endorsed by news media associations, in line with journalistic principles and processes.

- The signatories recognise the ongoing legislative work to develop standards for transparency about the main parameters of ranking included in the draft Platform to Business Regulation as well as the work being carried out by the EU Artificial Intelligence Expert Group as well as the EU consumer acquis ».

[119] Directive 2019/790/UE du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (texte présentant de l'intérêt pour l'EEE), PE/51/2019/REV/1, *J.O.*, L 130, 17 mai 2019, pp. 92-125.

techniques, affirme certes la Commission[120] mais on voit mal comment des « fournisseurs de services de partage de contenus en ligne » de taille importante, comme Facebook, Spotify, Google, …, pourront faire preuve de leurs efforts raisonnables de filtrer les contenus illicites sans recourir à des moyens technologiques. Le second point est d'exiger que les mesures techniques retenues de protection des œuvres, dont notamment mais pas uniquement celles de l'article 17 soient conformes au droit. Le considérant n° 7 de la directive de 2019 est clair : « La protection des mesures technologiques prévue dans la directive 2001/29/CE reste indispensable pour assurer la protection et l'exercice effectif des droits conférés aux auteurs et aux autres titulaires de droits en vertu du droit de l'Union. Il convient de maintenir cette protection, tout en veillant à ce que l'utilisation de mesures technologiques n'empêche pas les bénéficiaires de jouir des exceptions et *limitations* prévues par la présente directive ». Ce principe général de conformité des solutions technologiques aux dispositions légales est souligné amplement à propos des mesures qui seraient prises en vertu de l'article 17 : « Les mesures prises par les fournisseurs de services de partage de contenus en ligne en coopération avec les titulaires de droits ne devraient pas avoir pour conséquence d'empêcher la disponibilité de contenus qui ne portent pas atteinte au droit d'auteur, y compris d'œuvres ou d'autres objets protégés dont l'utilisation est couverte par un accord de licence, ou par une exception ou une limitation au droit d'auteur ou aux droits voisins. Les mesures prises par ces fournisseurs de services ne devraient, dès lors, pas affecter les utilisateurs qui utilisent les services de partage de contenus en ligne afin de téléverser de manière licite des informations sur ces services et d'y accéder de manière licite » [121]. Il s'agit bien

[120] Sur ce point, la Commission européenne a été très claire dans sa fiche d'information publiée le 26 mars 2019 : « Les nouvelles règles n'imposent pas d'utiliser des filtres de téléchargement. Elles n'imposent pas non plus aux plateformes de mise en ligne de contenus par les utilisateurs d'appliquer une technologie spécifique de reconnaissance des contenus illicites. En vertu des nouvelles règles, certaines plateformes en ligne seront tenues de conclure des accords de licence avec les titulaires de droits – par exemple, des producteurs de musique ou de films – pour pouvoir utiliser des œuvres musicales, des vidéos ou d'autres contenus protégés par le droit d'auteur. En l'absence d'accords de licence, ces plateformes devront faire tout leur possible pour s'assurer que les contenus non autorisés par les titulaires de droits ne sont pas disponibles sur leur site web. L'obligation de « faire tout son possible » n'impose aucun moyen ni aucune technologie spécifique ».

[121] Considérant n° 66. Le texte de l'article 17.7 transcrit ce principe : « La coopération entre les fournisseurs de services de partage de contenus en ligne et les titulaires de droits ne conduit pas à empêcher la mise à disposition d'œuvres ou d'autres objets protégés téléversés par des utilisateurs, qui ne portent pas atteinte au droit d'auteur et aux droits voisins, y compris lorsque ces œuvres ou autres objets protégés sont couverts par une exception ou une limitation. Les États membres veillent à ce que les utilisateurs dans chaque État membre puissent se prévaloir de l'une quelconque des exceptions ou limitations existantes suivantes

d'affirmer le rôle de la technologie mais de rappeler que les balises de son intervention sont bien fixées par la loi. Il n'empêche : c'est aux pouvoirs privés que la directive confie le soin de déterminer les moyens de respecter la loi et il est loin d'être acquis que l'autorité publique pourra contrôler le respect de telles exigences.

Conclusions

35. P. Martens, déjà cité, nous invitait à retrouver, à l'ère du numérique et de la transparence, les vertus du secret : « N'est-elle (la société) pas prête, écrivait-il, à troquer le secret contre la valeur inverse de la transparence ? Déjà, on assiste à une inversion chronologique. Naguère, le secret étant premier, la transparence était une conquête sur la privatisation de la connaissance. Aujourd'hui c'est l'inverse et le triomphe du non secret ne cesse de s'étendre : l'utopie de la transparence est légitime lorsqu'il s'agit de percer les secrets excessifs de l'État, de l'administration et, plus généralement des puissants et des pouvoirs. Mais dès lors qu'elle cesse d'être un moyen pour devenir une fin, qu'elle exige de percer les secrets des particuliers, elle devient un mode d'investigation des personnes. Elle rend tout secret illégitime. Elle se confond avec la légalité. L'absence de transparence est elle-même un chef d'accusation grave : elle renverse le fardeau de la preuve puisqu'elle impose de rendre des comptes *a priori*. Elle réalise le Panopticon, qu'elle entend étendre à l'ensemble de la société. Elle annonce l'avènement de la transparence totalitaire : alors que la dictature ne cherche qu'à détecter ses ennemis, le totalitarisme veut tout savoir sur tout le monde, pour pouvoir tout contrôler, y compris dans ses propres rangs ».

Ces réflexions invitent à un débat éthique et sociétaire. Comment repenser l'équilibre entre transparence et secret à l'heure où le numérique renforce les potentialités de l'une et l'autre valeur et cherche à mettre le droit tantôt au service de l'une, tantôt de l'autre ? L'analyse horizontale proposée à travers divers domaines du droit : le droit administratif, le droit des libertés, le droit professionnel, le droit pénal et le droit de la propriété intellectuelle témoignent dans chacun de ces domaines de l'ambivalence du droit, de sa référence à des concepts vagues qui de plus en

---

lors du téléversement et de la mise à disposition de contenus générés par les utilisateurs sur les services de partage de contenus en ligne : a) citation, critique, revue ; b) utilisation à des fins de caricature, de parodie ou de pastiche ».

plus laissent aux juges le soin de trancher, de peser, à l'aune de la proportionnalité[122], les intérêts qui se cachent derrière les dogmes tant de la transparence que du secret. La tâche du juge sera particulièrement délicate quand après avoir affirmé la valeur prônée *a priori* par la loi, cette même loi énonce des exceptions proclamées au nom d'autres valeurs, comme nous l'avons vu dans la loi sur l'accès aux documents administratifs ou en matière de secret d'affaires. En matière d'accès aux documents administratifs, c'est la transparence qui est érigée en principe alors qu'à l'inverse, dans la directive sur le secret d'affaires, c'est le principe du secret qui prévaut. Devra-t-il considérer que, selon les règles traditionnelles d'interprétation juridique, l'exception est de stricte interprétation ou, au nom de la valeur que l'exception exprime, lui accorder une égale valeur à celle affirmée par le législateur ?

36. Sans doute, la question de la démocratie ou pour être plus précis, la démocratie participative ou la possibilité pour chacun réellement informé de prendre part à la discussion publique implique l'accès du citoyen aux données collectées ou traitées par l'État et l'administration au sens le plus large du terme[123], elle justifie que les dérogations de la législation relative aux secrets d'affaires soient entendues de manière large et on souligne à cet égard le devoir renforcé de transparence des entreprises vis-à-vis des autorités. Sans doute, l'attention récente portée aux lanceurs d'alerte s'inspire-t-elle de la même volonté de transparence à la suite de débats publics autour des faits de fraude et d'illégalités[124] ? Le « dogme de la transparence », selon Jennifer Marchand, « a fait naître une exigence de la société civile à l'égard des secteurs public et privé : l'obligation de justifier du caractère raisonnable de leurs actions : l'« *accountability* ». La société de la transparence a suscité une vigilance accrue des citoyens : l'« *answerability* » ou le droit d'exiger des comptes »[125].

---

[122] À cet égard, sur ce principe qui doit arbitrer les conflits entre libertés, la thèse de Th. LEONARD, *Conflits entre droits subjectifs, libertés civiles et intérêts légitimes*, Bruxelles, Larcier, 2005. Plus récemment sur la montée des conflits entre libertés à l'heure du numérique, lire S. TURGIS, « Les droits de l'homme à l'heure d'internet et du numérique : rupture ou continuité ? », in *L'Europe des droits de l'Homme à l'heure d'Internet* (C. DE TERWANGNE et Q. VAN ENIS dir.), Bruxelles, Bruylant, 2019, pp. 65 et s.

[123] Sur ce point, lire D. CUSTOS (dir.), *La transparence, un principe de gouvernance*, Actes du XII[e] Congrès de l'Association internationale de méthodologie Juridique, Bruxelles, Bruylant, 2014 et A. BOUVIER, « Démocratie délibérative, démocratie débattante, démocratie participative », *Revue européenne des sciences sociales* [en ligne], XLV-136, 2007, pp. 5-34.

[124] En ce sens, les remarques d'A. LACHAPELLE, « La protection des lanceurs d'alerte », *op. cit.*, n° 25.

[125] J. MARCHAND, « Le droit d'alerter, entre transparence et secret », *La Revue des droits de l'homme* [en ligne], 2016/10, p. 3.

La démocratie n'a-t-elle pas également été invoquée pour justifier le double mouvement de notre réglementation de la vie privée ? cette réglementation apparaît, d'une part, comme une exigence accrue de transparence des responsables de traitement de données et des flux de données et lutter, ainsi, contre la transparence unilatérale que le numérique crée au profit de ce dernier et, d'autre part, comme une consécration du droit de ne pas apparaître, de rester secret ? Il s'agit bien là de reconnaître – et notre civilisation du numérique et de la transparence unilatérale l'exige – les deux conditions pour que chaque citoyen puisse développer sa personnalité et participer pleinement à la vie sociétaire et démocratique. Garder des zones d'ombre et de retraite pour l'individu, garantir par le secret du dialogue, la confiance envers des confidents nécessaires constituent une exigence de survie de nos personnalités dans notre monde de la technologie de surveillance ubiquitaire.

L'appropriation croissante qu'autorise le numérique en matière de propriété intellectuelle soulève également la question de l'accès de tous au savoir : comme l'affirme le Sommet Mondial de la Société de l'Information, « [c]hacun devrait avoir la possibilité d'acquérir les compétences et les connaissances nécessaires pour pouvoir jouer un rôle actif dans la société de l'information… »[126]. La création d'un espace public informationnel enrichi par les contributions volontaires des auteurs dans le cadre des mouvements *OPEN* apparaît dès lors comme une nécessité.

37. Ainsi, l'exigence démocratique ou plutôt notre conception de la démocratie à définir ou en tout cas à préciser au regard de ces deux valeurs semble bien être le *leitmotiv* du débat que ce colloque me proposait d'ouvrir. Notre démocratie, sans une action décidée en sa faveur, est menacée par la puissance et la domination qu'elle confère aux géants du net tant vis-à-vis des citoyens que vis-à-vis des États. L'État lui-même est tenté d'utiliser l'outil pour multiplier la surveillance des citoyens, sécurité oblige. Les risques de manipulations de l'opinion publique que le scandale *Cambridge Analytica* a révélés et de désinformations de celle-ci constituent d'autres dangers. Enfin, l'opacité des réseaux et de leur fonctionnement fait craindre une attitude de plus en plus conformiste des individus et la disparition des solidarités traditionnelles. Sans doute, le débat est-il trop sérieux pour le laisser au seul juriste ! Que l'autorité publique convoque, autour de ce débat à multiples facettes, les représentants des divers groupes d'intérêts, sans oublier les associations de libertés

[126] SMSI, *Déclaration de Principes*, Genève 2003, n° 29. La déclaration (n° 32) en appelle d'ailleurs aux créateurs, éditeurs et auteurs de contenus, invités à contribuer à promouvoir la société de l'information (inclusive).

civiles, de consommateurs, le monde professionnel, la Commission de protection de la vie privée, etc. Que tous ces groupes entendent les experts du numérique qui pourront leur préciser les potentialités, les risques, les enjeux de ses applications. En effet, dans ce débat, la technologie n'est pas neutre : elle peut pousser à telle ou telle dérive, elle peut également favoriser, comme nous l'avons montré à propos de chacun des thèmes, des solutions plus adéquates à l'objectif poursuivi. Il s'agira donc, dans le débat éthique auquel doit être confié le soin de peser les vertus contradictoires de la transparence et du secret ou dit autrement de balancer entre « Ombres et Lumières », d'inviter la technologie, non comme un ennemi mais comme un partenaire[127]. Si la technologie constitue le problème, elle en offre également la solution. Sans doute, n'est-ce pas à elle de définir le contenu de la norme. Pour paraphraser L. Lessig « le Code (entendre le code digital) ne doit pas être loi », certes mais si on n'y est pas attentif, il pourrait le devenir, comme il a été reconnu en matière de DRMS où la technologie pourrait bien définir un nouveau droit d'auteur renforcé. Le rôle de la technologie n'est pas de créer de nouvelles normes mais, dans les limites de la reconnaissance légale qui fixe le contenu de la norme, son rôle limité mais certain est d'en garantir une meilleure effectivité. On ajoute que la logique qui préside aux applications technologiques, en particulier lorsque leur utilisation affecte les personnes concernées (droit de la protection des données[128]) ou leur accès à l'information (transparence administrative ou propriété intellectuelle[129]), doit être transparente et pouvoir être comprise voire contestée par ces derniers. La « contestabilité » de la norme est le propre de la norme juridique, ne doit-elle pas s'imposer également à la norme induite par le numérique. Elle constitue, à notre sens, une condition de survie de nos libertés et de notre démocratie ?

C'est à ces débats éthiques essentiels pour le devenir de notre démocratie, que l'invitation du REHNAM à débattre aujourd'hui de ce difficile équilibre entre ombres et lumières, nous renvoie. Que votre association, Monsieur le Président, Pierre Devos, soit remerciée de cette initiative.

---

[127] Sur ce thème, notre ouvrage, *La « révolution » numérique – Quelle place encore pour le Droit*, Collection, L'académie en poche, février 2020.

[128] Voy. *supra*, n° 15.

[129] Ainsi, les mesures techniques de protection des œuvres devraient être transparentes lorsqu'elles sont opposées à un utilisateur ou candidat utilisateur (*supra*, n° 29).