INTERNATIONAL JOURNAL OF **DIGITAL AND DATA LAW**

REVUE INTERNATIONALE DE DROIT **DES DONNÉES ET DU NUMÉRIQUE**

ISSN 2553-6893

IMODEV
LES ÉDITIONS

Vol. 8 - 2022

International Journal of Digital and Data Law
Revue internationale de droit des données et du numérique

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6893

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

Les propos publiés dans cet article n'engagent que leur auteur.

The statements published in this article are the sole responsibility of the author.

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -

CC-**BY-NC-ND**

Attribution
Pas d'utilisation commerciale – Non Commercial
Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale de droit des données et du numérique (RIDDN)/ the International Journal of Digital and Data Law** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV. Enfin, associée de BeRecht Avocats, elle est avocate au barreau de Paris et médiateure professionnelle agréée par le CNMA.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV. Fondateur et associé de BeRecht Avocats, il est avocat au barreau de Paris et médiateur professionnel agréé par le CNMA.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons CC-**BY-NC-ND** :

1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;

2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Digital and Data Law / Revue Internationale de droit des données et du numérique (RIDDN)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV. Partner at BeRecht Avocats, she is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV. Founder and partner at BeRecht Avocats, he is an attorney at law at the Paris Bar and a professional mediator accredited by the CNMA.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license CC-**BY-NC-ND**:

1) the *International Journal of Open Governments*/ la *Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

2) the *International Journal of Digital and Data Law* / la *Revue internationale de droit des données et du numérique* (RIDDN) [ISSN 2553-6893].

L'HOMME INVISIBLE À L'ÈRE NUMÉRIQUE : DU MYTHE À LA RÉALITÉ CONTEMPORAINE

par **François VIANGALLI**, Maître de conférences à l'Université Grenoble-Alpes CESICE, Grenoble Cybersecurity Institute.

L'objet du présent travail est de s'interroger, à l'heure de la surveillance de masse, sur la légitimité d'un hypothétique *droit à l'invisibilité* numérique. Il expose l'origine de ce questionnement, son étendue ainsi que la réponse précise que, selon nous, il appelle.

L'invisibilité enflamme depuis toujours l'imagination des hommes. De Platon à Wells, en passant par Tolkien, il n'est de philosophie, littérature ou mythologie qui n'ait abordé la question. Fantasme littéraire ou pinacle de l'art de la guerre, l'invisibilité est un mythe philosophique autant qu'un idéal tactique. Mais, si dans les époques antérieures à l'essor des nouvelles technologies l'invisibilité se présente davantage comme une allégorie que comme une réalité technique, la situation pourrait bien changer à l'ère contemporaine. Ceci, pour deux raisons. La première est que certains outils numériques permettent, pour qui sait y accéder et en faire usage, de dissimuler les traces de sa présence et de son passage sur une partie du réseau. Autant il est difficile d'être physiquement invisible dans le monde réel, autant, dans le monde virtuel, cela est plus aisé[1]. La seconde raison est que le champ de vision offert par la technologie numérique dépasse en étendue celui de toutes les autres technologies qui l'ont précédé. A l'époque de l'Empire romain, il n'était évidemment pas possible à l'Empereur en personne de connaître l'opinion ou les habitudes de consommation des citoyens en temps réel par la collecte et l'analyse des données. Deux mille ans plus tard, il en était encore de même, en France et en Europe, avant l'avènement du web 2.0. Pour étudier l'opinion et l'« état de la société française », les personnes publiques et privées recouraient à des organes d'enquête pratiquant l'immersion réelle par l'envoi de chercheurs consignant *in situ* les us et coutumes des citoyens. La situation a radicalement changé. La collecte et l'analyse des données ont permis aux géants du numérique et aux États d'observer, plus que cela n'a jamais été possible, ce que font, ce que pensent et ce qu'expriment les citoyens. Le *champ de vision* s'est prodigieusement étendu. Internet est un *panoptique en réseau* où le concept même de vie privée est bouleversé. Si Bettelheim avait pu prophétiser le déclin de la vie privée à la fin des années soixante[2],

---

[1] À titre d'exemple, un réseau informatique comme I2P, se présente explicitement comme un projet de l'internet invisible : [www.geti2p.net] .

[2] B. BETTELHEIM, "The Right to Privacy is a Myth", *Saturday Evening Post*, July 27th, 1968.

nul n'avait prévu que celle-ci deviendrait à ce point vitale, à l'heure où l'observation est partout[3], et où le besoin de protection s'accroît. Les caractéristiques d'Internet le prêtent par nature à cette extension du champ de vision qui renouvelle entièrement la question de l'invisibilité.

Certes, le réseau Internet repose avant toute chose sur une infrastructure matérielle. Il n'y a pas d'internet sans *data center*, sans câbles sous-marins ni fibre optique terrestre, disque dur ou microprocesseur. L'information circulant en langage binaire, elle repose sur l'alimentation électrique et donc sur les échanges entre des appareils physiquement alimentés.

Mais l'internet se distingue aussi par son caractère intrinsèquement international, qui l'expose à une multilatéralité géographique de menaces. Alors que dans la plupart des situations de fait donnant lieu à un litige, la présence d'éléments d'extranéité constitue une complication adventice, le caractère international est extrêmement fréquent, pour ne pas dire quasi-systématique en présence d'un conflit relatif à l'usage de la technologie numérique, puisque la structure même d'internet repose précisément sur la mise en relation d'appareils à distance, tous potentiellement situés dans des zones différentes. Dès lors, l'internet apparaît comme le nouveau royaume du droit international privé.

Or ce caractère international rend possible l'observation du comportement d'autrui, à distance des frontières physiques, à partir d'un poste de scrutation situé sur un territoire où la réglementation du pays de la personne observée n'a pas cours. A l'instar du personnage du film d'Alfred Hitchcock *Fenêtre sur cour* (1954), qui observait la vie privée de ses voisins d'immeubles à l'aide d'une paire de jumelles, la technologie numérique permet l'*observation à distance* de nos us et habitus, en échappant en tout ou partie à la loi du pays dans lequel nous sommes. Cette observation, qui permet la collecte de données, puis leur analyse, en vue de la réalisation d'études de marché ou plus spécifiquement de diagnostic stratégique, fait que l'être humain n'a jamais été autant vu par ses semblables qu'il ne l'est aujourd'hui. Non seulement les États profitent de cette technologie pour observer une masse considérable d'internautes – parfois à leur insu comme Edward Snowden l'a révélé [4] - mais de surcroît les géants du numérique le font aussi à chaque seconde. Une bonne partie de l'activité du numérique est en effet basée sur l'économie de la data.

Cette observation du comportement d'autrui se traduit, après collecte, par l'écriture d'un code qui résume les traces pertinentes que l'internaute a laissées, et qui résument son activité. Or ce code, qui n'est donc pas à proprement parler une empreinte analogique, mais bien seulement un texte, un *gramma* comme auraient dit les

[3] Voir sur ce point notre entretien avec V. MAYER-SCHÖNBERGER, : *in* D. DÉCHENAUD (dir.), *Le droit à l'oubli numérique,* Larcier, 2015, p. 328.
[4] E. SNOWDEN, *Mémoires vives*, éd. Seuil, trad. E. Ménenteau & A. Blanchard, 2019.

Grecs[5], peut être dupliqué ès qualités une infinité de fois, en circulant avec une très grande facilité. En effet, les données collectées ne sont pas la trace physique laissée par la personne sur un support matériel – à l'instar d'une empreinte de pas dans la boue, d'une empreinte sonore sur une bande magnétique ou d'une impression lumineuse sur une pellicule de photographie argentique – mais seulement une *description par un texte* de ce que la personne a fait[6]. Or il est extrêmement aisé de faire circuler et de reproduire ce texte, quel qu'en soit le nouveau support, en usant des moyens de transmission électronique. Autrement dit, une fois que la personne a été vue, une partie de ce qu'elle a fait est consignée dans un texte qui peut désormais circuler de personnes étrangères en personnes étrangères, d'un pays à l'autre, sans même que l'intéressé ne puisse le savoir.

Il est connu que l'homme a besoin d'espace privatif pour s'abriter du regard d'autrui. La chose est souvent exprimée en France à travers la célèbre formule de la pièce de théâtre *Huis clos* de Sartre, dont l'un des personnages, prisonniers du regard permanent d'autrui et dépourvu à ce titre de véritable vie privée, s'exclame : « *L'enfer, c'est les autres* ». Mais elle est également démontrée empiriquement par les résultats catastrophiques de l'expérimentation des prisons construites sous la forme d'un *Panoptique*, tel que l'avait théoriquement conçu le philosophe anglais Jeremy Bentham. Pour Bentham, il apparaissait judicieux de construire une prison dans laquelle les cellules seraient disposées en cercle, au centre duquel un petit nombre de gardiens auraient pu avoir une vision à 360° de l'ensemble des détenus. De surcroît, dans ce modèle, tous les prisonniers auraient pu s'observer mutuellement, de cellules à cellules, puisque chacun des cachots aurait été fermé par une grille n'obstruant en rien la vue entrante ou sortante. Autrement dit, chaque prisonnier peut voir, et donc surveiller, tous les autres. Cette invention reposait en milieu carcéral, sur une certaine forme d'abolition de la vie privée. Or, précisément, l'expérience réelle démontra que c'était probablement la pire chose à faire. Les prisonniers, dans un tel établissement, devenaient littéralement fous. Privés d'espace reclus, leur santé mentale était gravement atteinte, au point que ce modèle carcéral fut abandonné. Si l'on devait tirer une leçon de cette expérience, il faudrait sans nul doute reconnaître que le besoin de *Privacy* est tout simplement vital chez l'homme. Se laisser observer en permanence n'est pas conforme à notre nature.

A l'ère du numérique, l'observation généralisée à distance par la collecte des données a pris une telle ampleur que la question de la visibilité de la personne, et désormais celle de son opposé, celle de l'*invisibilité*, se pose en des termes entièrement nouveaux. Puisque

[5] To gramma, atoς : la lettre, le texte ; voir A. BAILLY, *Dictionnaire grec-français*, 1895, p. 416
[6] Sur la distinction entre l'empreinte analogique et le résultat grammatique de la collecte de données, voir notre étude : *L'approche Big Data en droit international privé*, *in* A. FAVREAU (dir.), *La propriété intellectuelle en dehors de ses frontières,* Larcier, 2019, p. 200.

nous n'avons jamais été autant vus, y compris à notre insu, ne serait-il pas légitime de nous reconnaître un droit à ne pas être vu, c'est-à-dire, en conséquence, un *droit à l'invisibilité numérique* ? Pour répondre à cette passionnante question, il importe, à l'évidence, de définir préalablement l'invisibilité (§ 1), avant d'en tirer l'analyse juridique de son éventuel usage (§ 2).

§ 1 – QU'EST-CE QUE L'INVISIBILITÉ ?

L'invisibilité nourrit les mythes, contes et légendes depuis l'aube des temps. Les réflexions qui l'entourent en général ne sont pas fondamentalement nouvelles, si l'on excepte le cas particulier de l'invisibilité numérique de l'époque moderne.

A) De l'invisibilité en général

Pour aborder un tel sujet, il est impératif de s'entendre par convention sur l'objet exact du débat, afin d'en identifier les propriétés, et de parer aux dérivations que les mythes et légendes, tous riches qu'ils soient, ne manqueraient pas, à défaut, de susciter à l'esprit.

1) Précisions sémantiques

L'invisibilité personnelle peut être définie comme *la qualité d'une personne dont l'existence, la présence ou l'action ne peuvent être perçues d'autrui*. Se trouve ainsi présenter un caractère invisible la personne dont nul ne soupçonne l'existence ; ou, à un degré moindre, celle dont l'existence est connue mais dont la présence en un lieu précis et à un moment donné est imperceptible ; ou, à un degré moindre encore, celle dont l'existence et la présence sont perçues, mais dont les gestes, faits et actes sont imperceptibles. L'invisibilité est ainsi graduée, selon sa puissance d'occultation, mais elle revient toujours à évincer en tout ou partie le pouvoir de perception d'autrui.
Ainsi entendue, l'invisibilité se distingue de plusieurs notions qui lui sont proches.
Elle se distingue tout d'abord de l'*anonymat*. L'invisibilité est un genre d'occultation dont l'anonymat n'est qu'une espèce. En effet, le propre de l'anonymat est d'occulter l'identité véritable de la personne. L'anonymat n'est donc qu'une forme d'invisibilité : celle du nom. La personne anonyme ne dissimule pas nécessairement son existence, ni même sa présence. On peut être anonyme en portant ostensiblement un masque en public ; ou, au contraire, user de l'anonymat par l'envoi de missives ou la publication d'un texte en ligne sans signaler sa situation géographique. L'anonymat, en tant qu'invisibilité du nom, peut se conjuguer avec d'autres formes d'invisibilité ou se limiter à lui-même.
Elle se distingue ensuite de l'*invincibilité*. De prime abord, la distinction semble gratuite. Conceptuellement, les deux mots n'ont en commun que leur allitération. Pourtant, dans l'imaginaire

collectif, l'invisibilité évoque irrésistiblement une forme de pouvoir extraordinaire, qui rendrait son détenteur invincible et dangereux. En réalité, cette assimilation est largement fausse. Ceci pour une raison très simple : il n'existe pas d'invisibilité magique. La seule invisibilité qui puisse exister est celle découlant de l'emploi de procédés techniques propres à dissimuler le sujet considéré à autrui. Mais cette dissimulation obtenue par des moyens physiques peut être dissipée par les mêmes moyens physiques utilisés en sens inverse. Par ailleurs, sur les plans juridique et même éthique, il ne faut pas confondre l'invisibilité et le mésusage de celle-ci. Aucune loi n'impose à ce jour au citoyen de se promener dans la rue avec l'indication ostensible de son identité. Au milieu d'une foule, loin de ses fréquentations, un individu perdu dans une grande ville est déjà naturellement dans une situation d'invisibilité modérée. Il n'est pourtant nullement « invincible », et il ne viendrait à l'esprit de personne de l'accuser d'une quelconque imminente et mauvaise action du simple fait que son identité exacte n'est pas perceptible au premier regard. En d'autres termes, distinguer l'invisibilité de l'invincibilité a pour mérite de rappeler qu'une certaine forme ou un certain degré d'invisibilité personnelle sont tout à fait naturels en société, dans nombre de circonstances, outre que ladite invisibilité est réversible. La distinction a pour mérite de rappeler que la première n'est pas l'instrument de la seconde, contrairement à ce que la légende populaire suggère. Rester invisible, à un degré ou à un autre selon les circonstances, n'est pas en soi criminel.
L'invisibilité se distingue enfin de l'*impunité*. Si l'invisibilité ne mène pas nécessairement au crime, elle ne postule en aucun cas, lorsque cela advient malgré tout, une quelconque immunité. Ceci pour deux raisons. La première est que l'invisibilité ne constitue nullement une échappatoire juridique. Le fait d'être invisible ne soustrait pas le sujet, dans l'exercice de cette invisibilité, à l'autorité de la loi. La seconde raison réside dans le caractère réfragable de toute forme d'invisibilité. La dissipation du « sortilège » d'invisibilité n'est qu'une question de moyens techniques, pas une question de principe. Dès lors, non seulement l'invisibilité reste en soi neutre, car l'usage qui en est fait peut parfaitement être naturel et vertueux ; mais elle peut aussi, à l'inverse, démontrer l'intention de nuire de celui qui s'en sert dans un but déshonnête. Après sa réfraction, son usage peut démontrer, en effet, de façon certaine, la préméditation de l'auteur de faits condamnables.

2) Les propriétés de l'invisibilité

L'invisibilité se distingue par quatre propriétés fondamentales.
La première est d'être *relative*. L'invisibilité, si on la considère dans le monde réel et non dans l'imaginaire, est toujours limitée dans le temps, l'espace et le contexte.
Elle est relative dans le temps dès lors qu'elle suppose le recours à un artifice, ce qui est presque toujours le cas pour une personne.

Qu'il s'agisse pour cette dernière de se confiner à domicile en fermant porte et fenêtres, de se grimer le visage au milieu d'une foule, ou d'agir furtivement, l'action de rester invisible est nécessairement temporaire.

Elle est également relative dans l'espace, pour la simple raison qu'une chose ou une personne ne sont invisibles qu'à partir d'un certain point de vue. La réalité ne peut être occultée à la perception humaine ou au pouvoir de détection d'une machine que sous un certain angle et pour un type particulier de perception. Ainsi, par exemple, de la personne qui occulte le sens véritable de son discours, et rend son authentique message invisible, lorsqu'elle utilise un code. Dans ce cas, le sens réel de la communication est invisible pour le non-détenteur du code. Mais la communication en elle-même n'est pas dissimulée. De la même manière, la personne qui cache une arme blanche dans sa poche, par exemple un poignard minéral, pourra peut-être franchir au contrôle de sécurité le portique de la salle d'embarquement d'un aéroport, sans être repérée. Mais l'arme, invisible aux détecteurs de métaux, sera aisément découverte par une fouille personnelle. Sur un plan similaire, le tricheur qui se distribue une fausse main au poker n'est invisible aux yeux de ses victimes que parce qu'il exécute sa manipulation des cartes au moment précis où il sait ne pas être observé. Sans ce relâchement de l'attention des joueurs et la survenance d'une zone d'ombre dans la perception – ce que les tricheurs appellent le « *shade* » - la triche est impossible. Comme l'illustre parfaitement le tableau de Georges De la Tour, *Le Tricheur à l'As de carreau* (1635), c'est dans l'inattention des victimes que la triche prospère. L'invisibilité n'est pas totale : elle se limite à un angle de perception particulier, au cours d'un moment précis.

L'invisibilité est enfin relative au contexte qui est le sien. En réalité, il n'existe pas d'invisibilité absolue des personnes ou des choses humaines[7]. Dans la Cité, l'invisibilité du citoyen est toujours le résultat d'un compromis et d'un concours de circonstances. Il est certes possible de définir la vie en l'opposant absolument à la mort, à la façon de Xavier Bichat, pour qui « *la vie est l'ensemble des fonctions qui résistent à la mort* »[8]. Mais il est impossible d'en faire autant pour définir l'invisibilité sociale, pour la simple raison qu'il n'y a pas de rupture nette, infranchissable et définitive entre ce qui est visible à un moment précis et d'un certain point de vue, et ce qui ne l'est pas à un autre moment et sous un autre point de vue. La vérité réside plutôt, selon nous, dans un *continuum* reliant le visible à l'invisible, selon les instants et les circonstances. L'invisibilité absolue n'existe pas. Pour s'en convaincre, il suffit de considérer l'hypothèse contraire. Soit en effet une distinction absolue et étanche entre le visible et l'invisible dans le domaine de la perception strictement

[7] Notre exposé se limite à la question de l'invisibilité de la personne et de ses biens et actions en droit. Il relève par conséquent de la sphère sociale, et non des phénomènes naturels, biologiques ou physiques.

[8] Ph. HUNEMAN, *Bichat : la vie et la mort*, PUF, 1998, p. 5.

visuelle. A cet endroit, les deux opposés peuvent être désignés comme étant l'Ombre, d'une part, et la Lumière, d'autre part. Or, que voit-on dans l'Ombre totale ? Rien assurément. Mais que voit-on également dans la Lumière totale ? La réponse est encore la même : rien, assurément, car *dans la lumière totale, l'œil est aveuglé*. Personne ne peut rien voir dans la lumière absolue sinon un grand nuage blanc indépassable. La conclusion qui s'en infère est simple. Tout ce qui est vu n'est que *discerné* à partir de l'articulation de l'Ombre et de la Lumière. Le degré de discernement, et donc de perception d'une chose ou d'une personne, dépend de l'agencement des zones d'ombre et de lumière, et du point de vue retenu pour les observer dans le temps et dans l'espace. Cet agencement relatif n'est qu'une figure, à un instant précis, du continuum du visible et de l'invisible. En ce sens, l'invisibilité absolue de la personne et de ses actes n'existe tout simplement pas dans la Cité.

La seconde propriété de l'invisibilité réside dans son *caractère réfragable*. Tout procédé de dissimulation peut être réfracté, ou presque. Et s'il n'est pas possible de faire paraître ce qui a été dissimulé, il est à tout le moins possible de constater qu'une dissimulation a été organisée. Ce caractère réfragable peut sembler évident, puisque toute dissimulation est artificielle. Il mérite toutefois d'être souligné, dans une perspective précisément juridique. L'invisibilité à un moment précis n'exclut pas par principe l'identification ultérieure de la personne, pas plus que le constat de ses actes, dont elle répond en droit. Proscrire l'invisibilité en soi, au nom de l'efficacité de la surveillance et du respect de l'*imperium*, est en réalité un raccourci intellectuel.

La troisième propriété de l'invisibilité procède de sa *neutralité morale*. Contrairement à ce que suggèrent certaines représentations populaires ou littéraires, être invisible n'est ni bon ni mauvais en soi. Tout dépend de l'usage qui est fait de cet état. Ainsi, l'opposant politique à un tyran, qui utilise les techniques de dissimulation des communications pour entrer en contact avec la presse démocratique étrangère, n'est nullement à blâmer. A l'inverse, le trafiquant de stupéfiants qui écoule sa marchandise de façon dissimulée commet un crime. Dans les deux cas, l'invisibilité n'est ni le bien ni le mal, elle n'est que le vecteur d'une action qui seule peut être jugée.

La quatrième propriété de l'invisibilité ressort enfin de son *ambivalence tactique*. En tant qu'avantage, au sens stratégique du terme, elle peut être utilisée aussi bien dans un but défensif que dans un but offensif. Pour reprendre une métaphore du droit anglais des contrats, elle peut être employée comme un bouclier, autant que comme un glaive (« *as a shield or as a sword* ») [9]. A

[9] En droit anglais, l'institution du *promissory estoppel* permet en effet au débiteur actionné par son créancier en vue régler le montant total de sa dette – alors que celle-ci avait fait l'objet à titre gracieux d'une remise partielle, mais sans que ladite remise ne soit assortie de la contrepartie indispensable pour qu'elle acquière une valeur contractuelle –

l'évidence, le mode offensif suscite davantage de réserves – sauf son emploi par l'autorité légitime à des fins de police – que le mode défensif, si ce dernier sert tout simplement à protéger sa vie privée. La distinction mérite d'être faite, spécialement lorsque le régime juridique des diverses invisibilités vient à être défini.
Ainsi, il appert que l'invisibilité procède du caractère occasionnel d'une chose ou d'une personne, Elle ne présente en soi rien qui ne soit déjà connu d'une manière ou d'une autre. En la matière, c'est l'imagination des hommes qui a confisqué le débat en l'absolutisant. Mais concevoir l'invisibilité absolue à l'échelle humaine sous une perspective juridique n'a aucun sens, dans le monde réel. Un tel biais constituerait le meilleur moyen de compromettre l'impartialité d'analyse, et de laisser les représentations imaginaires d'une invisibilité irréelle perturber le sens de la justice. Or ces représentations sont si séduisantes pour l'esprit que leur influence, à l'accepter, en devient immédiatement palpable. Les connaître reste le meilleur moyen de les maintenir à leur place : celle des mythes.

3) Mythes et histoire

De l'Antiquité à nos jours, l'invisibilité a capturé l'imagination des hommes. Disons-le tout de suite : elle a rarement eu bonne réputation, et son usage a presque toujours été regardé comme le symbole du mal, de l'*hubris*, voire de l'assassinat.
Pour autant, il n'est pas inutile de parcourir brièvement l'histoire mythologique qu'elle a engendrée, car les réactions instinctives que suscite son emploi contemporain dans le monde numérique pourraient bien découler de cette forme d'inconscient collectif qui détermine – à tort selon nous – une lecture essentiellement criminelle de l'invisibilité. C'est pour récuser ce biais qu'il est sage d'en connaître l'origine.
Le texte le plus célèbre sur l'invisibilité est celui de Platon. Dans le livre II de la *République*, Platon évoque en effet le cas de Gygès de Lydie, un berger illettré qui vient à découvrir dans une crevasse un mystérieux cadavre qu'il s'empresse de dépouiller, à rebours de toute décence. Parmi les reliques, Gygès prend notamment possession de l'anneau qu'il retire du doigt du défunt. Tandis qu'il le manipule, Gygès comprend que l'anneau est en réalité un objet magique. Lorsque le chaton en est tourné vers l'intérieur, son porteur devient invisible. Gygès décide d'user de ce pouvoir pour commettre divers forfaits, et notamment se rendre à la cour du Roi, pour finalement l'assassiner après avoir séduit sa femme. Gygès

d'invoquer en *Equity* sa bonne foi et le manquement à la parole donnée par le créancier, pour faire échec à une telle demande. Cette réprobation à l'encontre de la parole donnée, même sans valeur contractuelle, n'est cependant admise qu'à titre défensif, et non à titre offensif pour réclamer de l'argent à un débiteur. On dit que le *promissory estoppel* ne peut être employé que « *as a shield and not as a sword* » : *Combe vs/ Combe* (2015) 2 KB 2015. Cette distinction entre l'admission à titre défensif d'une dérogation aux autres règles, et son admission, fort différente, sur le plan éthique, à titre offensif, nous paraît ici pertinente.

devient ainsi roi lui-même, par le crime et l'impunité. Platon évoque ce récit, par la bouche de Glaucon, son frère, pour exposer qu'il est difficile à un homme de résister à la tentation du mal, lorsqu'il a l'assurance d'échapper à la garde, à la justice et aux hommes en général. La justice n'est pas innée à l'individu, elle procède pour Platon de la contrainte qu'exercent les autres sur lui. Comme l'invisibilité suspend celle-ci, toute personne, même le Juste, finirait par commettre le crime, si l'anneau de Gygès lui était confié.
Platon écrit ainsi :

> « Si donc il existait deux anneaux de cette sorte, et que le Juste reçût l'un, l'Injuste l'autre, aucun, pense-t-on, ne serait de nature assez adamantine pour persévérer dans la justice et pour avoir le courage de ne pas toucher au bien d'autrui, alors qu'il pourrait prendre sans crainte ce qu'il voudrait sur l'agora, s'introduire dans les maisons pour s'unir à qui lui plairait, tuer les uns, briser les fers des autres et faire tout à son gré, devenu l'égal d'un dieu parmi les hommes. En agissant ainsi, rien ne le distinguerait du méchant : ils tendraient tous les deux vers le même but. Et l'on citerait cela comme une grande preuve que personne n'est juste volontairement, mais par contrainte, la justice n'étant pas un bien individuel, puisque celui qui se croit capable de commettre l'injustice la commet »[10].

Le discours sur la justice apparaît comme le véritable sujet de ce passage, indéniablement. Il s'agit de définir la justice et de récuser l'idée d'une vertu individuelle et sans contrainte. Mais l'invisibilité, quoiqu'elle ne soit ici que pure métaphore, ne s'en trouve pas moins marquée du sceau de l'infamie. Ce sceau, pour l'essentiel, va la poursuivre à travers les âges.
L'autre texte le plus célèbre sur l'invisibilité est bien sûr le roman de Herbert George Wells, *L'Homme invisible*. Paru en 1897, le roman raconte l'histoire d'un savant de génie appelé *Griffin* – ignoré de ses contemporains et passablement misanthrope – qui parvient à synthétiser une substance chimique dont l'absorption rend la personne invisible. Après avoir essayé avec succès le breuvage sur un chat, Griffin décide de l'expérimenter sur lui-même. Devenu invisible, sans possibilité de retourner à l'état normal, il va peu à peu, tel Gygès, lever une à une toutes ses inhibitions morales. Il commence par commettre de menus larcins, avant d'administrer quelques corrections aux personnes l'ayant mal reçu ou considéré. Contraint de se recouvrir entièrement le corps et le visage à la façon d'un grand brûlé, afin de pouvoir interagir socialement avec autrui sans dévoiler son intime secret, il suscite par son apparence curieuse un certain malaise en société. Ce malaise aiguise sa misanthropie et aggrave sa course vers le mal. C'est ainsi qu'il en vient à projeter l'assassinat d'un de ses anciens collaborateurs, et même à se proclamer « *Invisible Ier* », jugeant que son état le soustrait

[10] PLATON, *La République*, éd. Livre II, 360a. Trad. G. Leroux, Garnier-Flammarion, 2016.

désormais à l'autorité de la Reine. Sa folie sans limite le mène à l'imprudence, et les habitants du village où l'assassinat doit avoir lieu réussissent finalement à le saisir et à le lyncher. Son corps inanimé redevient alors visible, tandis que le recueil de ses notes, qui comprennent la formule du breuvage de l'invisibilité, est recueilli par Marvel, un ancien comparse devenu propriétaire d'une auberge grâce à de l'argent précédemment volé. Comble de l'ironie, Marvel est incapable d'en saisir le sens, puisque les notes sont incomplètes et qu'elles sont écrites en latin, en grec et en langage mathématique, définitivement impénétrables à l'esprit de leur nouveau possesseur.

Là encore, il est évident que Wells décrit l'effondrement moral que l'invisibilité engendre dans l'esprit de la personne, le pouvoir terrible qu'elle confère à son utilisateur et la fin tragique que la corruption lui réserve. A l'instar de Platon, Wells la conçoit sous la perspective criminelle, addictive et corruptrice. Il ajoute toutefois une dimension proprement juridique. Le délire du personnage, qui va se proclamer lui-même *« Invisible Ier »*, n'étant plus ès qualités sujet de la Reine, lui donne l'occasion de soulever la question de l'autorité de la norme lorsque le sujet s'efface[11]. Mais c'est là un mythe, une fois de plus. Toute invisibilité est réfragable, et le véritable problème n'est pas l'invisibilité en soi, mais le caractère irréversible qu'elle présente dans le récit. En réalité, Wells aborde ici, de façon implicite, la question de la réfraction : tant que l'invisibilité est réversible, Griffin reste un sujet de droit. Il rend compte de ses actes après réfraction. A l'inverse, là où la réfraction n'est plus possible, l'invisibilité mène irrémédiablement au crime, à l'isolement et à la folie. Enfin, l'illustre écrivain relève ce qui pourrait être qualifié de « *paradoxe de l'invisibilité* », à savoir le fait que, à rebours du sens commun, une personne invisible, si elle ne trahit pas son identité, attire néanmoins davantage l'attention qu'une personne ordinaire lorsqu'elle agit, car son action apparaît sans auteur ni explication. Lorsque Griffin soulève une tasse de café, le spectacle qui s'offre à autrui est saisissant : aux yeux d'un homme normal, la tasse « lévite » et s'incline toute seule. Voilà la raison pour laquelle le personnage de Wells est en réalité obligé de se recouvrir le corps ; car s'il use de son pouvoir pour s'enrichir, voler et tuer, il a néanmoins un besoin vital d'agir en société, et donc d'être vu comme n'importe qui. Ce « *paradoxe de l'invisibilité »* est particulièrement applicable à l'ère numérique. Plus un individu dissimule ses traces informatiques, plus paradoxalement il attire la

[11] H.L.A. Hart a relevé l'un des caractères de la norme juridique : sa persistance à travers le temps, nonobstant la disparition physique de celui qui l'a émise, et qu'il nomme *Rex* : H.L.A. HART, *The Concept of Law,* Oxford University Press, 1961, pp. 61 et s. Il semble que la question de l'invisibilité pose également celle de la persistance de la règle *en dehors du champ de vision* de Rex. Pour notre part, nous inclinons à penser que cette persistance est acquise pour une raison très simple : tout état d'invisibilité est temporaire et sera immanquablement réfracté s'il n'a expiré lui-même. Et comme l'invisibilité n'est pas l'impunité, la norme n'a nullement perdu de son autorité et s'applique au sujet et aux actes qu'il a accomplis en état de discrétion.

curiosité sur lui, puisqu'il en vient à agir davantage comme un individu suspect, et non comme l'homme du commun, résolument ignorant de l'art de la discrétion numérique. En cela, l'œuvre de Wells fournit une lecture tout à fait valable, à l'ère contemporaine, de l'invisibilité.

Enfin, l'œuvre de Tolkien offre la plus récente illustration romanesque, mythique et philosophique de l'invisibilité. Dans son œuvre maîtresse, *Le Seigneur des Anneaux*, paru en 1954, le Professeur d'Oxford décrit un univers menacé par le pouvoir maléfique d'une puissante divinité, Sauron. Le pouvoir de Sauron s'incarne dans le monde considéré, la *Terre du Milieu*, par le biais d'un anneau maudit, dont l'une des propriétés est précisément de rendre son porteur invisible. Ce pouvoir a le don d'attiser la convoitise extrême et de corrompre l'âme de celui qui le détient. Pour sauver la Terre du Milieu, la seule issue est de détruire l'anneau, ce qui requerra une lutte sans merci pour le protéger de la folie des hommes qui, tôt ou tard, en viennent presque tous à en convoiter la possession pour détenir son pouvoir. Ce n'est que lorsque l'anneau d'invisibilité est finalement détruit que Sauron, resté lui-même invisible tout au long de la guerre, est définitivement chassé.

Même si l'invisibilité n'est pas le thème exclusif de la saga de Tolkien – à la différence du roman de Wells – il est évident qu'elle occupe une place centrale dans la représentation du Mal et du terrible pouvoir qu'elle confère à celui qui en use. A nouveau, elle sert d'illustration au crime, à l'horreur et à la menace pour l'équilibre du monde. Le succès considérable du roman va par conséquent contribuer, après Platon et Wells, à ancrer l'idée que *l'invisibilité est avant tout le mal*.

Au-delà de la philosophie et de la littérature, l'idée d'invisibilité est également présente dans un domaine où, cette fois, elle représente le sommet de l'art : celui de la stratégie. Dans l'art de la guerre, l'invisibilité est l'arme absolue. Même si les hommes ne sont évidemment jamais parvenus à l'invisibilité parfaite, qui n'existe que dans les mondes imaginaires, la recherche de la discrétion ou de l'invisibilité partielle de la personne ou de ses actes occupe une place très importante. L'exemple le plus connu, dans l'Antiquité, est celui des Sicaires. Ces assassins zélotes exécutaient par surprise à la dague, au milieu d'une foule, des officiers romains, au Ier siècle après Jésus Christ, avant de disparaître dans la masse, fort d'un art consommé de la discrétion. Ces inventeurs de ce l'on appelle aujourd'hui *l'assassinat furtif*[12], fondaient leur stratégie de terreur, destinée à déstabiliser le pouvoir romain en Palestine, sur leur aptitude à disparaître dans la foule. Plus tard, au XIème siècle, la Confrérie des Assassins, un mouvement religieux ismaélien, dit *nizarite*, issu de l'islam, reproduira le même type de stratégie pour

[12] D. TAYLOR, Y. GAUTRON, in R. D. LAW (ed), *The Routledge History of Terrorism,* Routledge, 2015, p. 18.

déstabiliser le Califat des Abbassides, puis les Croisés[13]. L'art de l'assassinat, ou tout simplement du recueil furtif de renseignement, sera tout autant cultivé au Japon, entre le XVème et le XVIIème siècle[14]. D'une manière générale, la discrétion la plus grande est restée de tous temps l'arme absolue des États, et les services de renseignement contemporains continuent bien évidemment à en faire usage.
Il n'est pas question ici de dresser ici une brève histoire de l'invisibilité dans la philosophie, la littérature ou l'art de la guerre, fors tout regard juridique. D'autres, experts en la matière, s'y sont déjà livrés, au moins partiellement[15]. L'objet de notre propos, ici, est simplement d'expliquer pourquoi, culturellement, la réaction première à l'idée même d'invisibilité reste l'hostilité. Notre fonds commun de pensées, nos représentations et nos intuitions sont déterminés par cet héritage particulièrement critique à l'égard de ce type de pouvoir. Pourtant, à l'ère de la technologie numérique, la situation pourrait bien changer.

B) De l'invisibilité numérique en particulier

L'invisibilité numérique ne peut être comprise que par la compréhension préalable de l'espace dans lequel elle a vocation à s'exercer. Le cyberespace n'a pas en effet, les mêmes propriétés que l'espace physique, et il ouvre la voie à une surveillance des citoyens telle que l'histoire n'en a jamais connu auparavant. C'est bien pour cela que des techniques d'invisibilité ont été élaborées, dont il peut être fait usage ou mésusage.

1) Les propriétés du cyberespace

Le cyberespace peut être défini comme l'ensemble des échanges d'informations réalisés par numérisation et transfert à distance de machine à machine. A ce titre, il comprend bien évidemment les opérations informatiques réalisées sur le réseau de l'internet mondial, qui en constitue la partie la plus connue et la plus visible. Ainsi entendu, le cyberespace se compose de plusieurs couches, dont la réunion détermine son fonctionnement.
La première d'entre elles est la couche physique. Elle se compose des machines réceptrices et émettrices d'information, des centres de stockage de l'information (*Data centers*), et des appareils de liaison et transmission de l'information sous forme numérique, telles que les câbles terrestres ou sous-marins, les répéteurs

[13] B. LEWIS, *The Assassins, A Radical Sect in Islam,* Weidenfeld & Nicolson History, 2003 ; C. MILLIMONO, *La Secte des Assassins, Des martyres islamiques à l'époque des Croisades,* L'Harmattan, 2009.
[14] Voir ainsi les travaux du fondateur de l'hoplologie scientifique moderne – littéralement la science des armes – et spécialiste du Japon : D. F. DRAEGER, *The Art of Invisibility,* Lotus Press, 1977.
[15] Voir ainsi E. BARENDT, *Anonymous Speech : Literature, Law and Politics*, Hart Publishing, 2016.

optiques, les antennes et émetteurs d'ondes, *wifi* ou autres. Cette infrastructure, à l'importance stratégique cruciale à l'ère contemporaine, est la condition *sine qua non* du fonctionnement du cyberespace. Une attaque sur un seul des composants peut paralyser un opérateur, et une attaque sur un composant majeur, tel que le câble ou un data center, peut compromettre la sécurité de l'ensemble du système.

La seconde couche est la couche numérique. D'un point de vue physique, l'information circule à travers les câbles sous la forme de signal électrique ou lumineux, selon les cas. Et les antennes et émetteurs propagent quant à elles des ondes. Mais leur émission ou circulation se fait en alternant deux signaux, positif ou négatif, selon qu'il y a émission ou coupure de l'émission à un instant précis. A partir de cette alternance, un langage binaire permet de coder un message initialement conçu en langage humain naturel, en assignant à chaque combinaison de 0 et de 1 une signification alphabétique ou mathématique. La couche numérique ne procède donc pas, en amont, de l'émission du signal en soi, qui n'est qu'une composante de la couche physique, puisque l'électricité et la lumière, par exemple, sont bien des phénomènes physiques. Elle découle, en aval, de l'interprétation qui en est faite par convention humaine. *Autrement dit, l'information numérique est fondamentalement un phénomène linguistique.* C'est bien un langage qui est constitué, nonobstant son vecteur, qui n'est plus ni le pharynx ni la plume, mais pour l'essentiel l'électricité ou la lumière. Cette précision est importante, non seulement pour comprendre la structure du cyberespace en général, mais aussi pour l'appréhender au plan juridique. Les échanges numériques étant par nature des phénomènes linguistiques, nombre de questions qu'ils suscitent doivent avant tout être envisagées sur le terrain de la langue, c'est-à-dire du statut de celle-ci, de sa liberté d'usage ou de son détournement – l'on songe ici à la cryptographie – du contrôle ou de l'absence de contrôle de l'État, de la portée juridique de ses expressions, etc.

La troisième couche est la couche économique. Le cyberespace a engendré une gigantesque économie, devenue mondiale. Celle-ci peut être distinguée en deux parties. La première est celle qui se greffe sur l'économie réelle. Le cyberespace remplit alors sa fonction la plus simple de communication. Au lieu par exemple d'échanger les consentements de gré à gré et face à face, ils peuvent l'être à distance à un degré de rapidité et de facilité décuplées. L'exécution du contrat peut également en être simplifiée et optimisée, puisque les instructions linguistiques qui président à celle-ci passent par un vecteur plus rapide. La seconde partie de l'économie numérique est celle qui découle du fonctionnement du cyberespace. Ici, deux sous-groupes se divisent. L'un concerne l'économie du cyberespace proprement dit, c'est-à-dire la richesse créée par l'entretien et le développement de la couche physique. L'autre sous-groupe concerne l'économie autonome que le

cyberespace engendre en constituant par lui-même des actifs qui, en tout ou partie, n'ont de valeur qu'à travers lui. Les cryptomonnaies sont l'exemple topique de cette cyberéconomie autonome.
Enfin, la quatrième couche est la couche juridique. Contrairement à ce que l'utopie libertaire des débuts de l'internet avait souhaité, le cyberespace est aujourd'hui très largement réglementé. Non seulement les États le réglementent, mais même ils le surveillent. Penser qu'internet puisse maintenir au-delà de l'orbite des systèmes juridiques étatiques, et surtout qu'il y subsiste une forme d'anarchie ou d'impunité, est une parfaite illusion. A dire vrai, c'est même précisément parce que l'empire du droit s'y est imposé, avec une puissance de surveillance jamais atteinte, que la question d'un droit à l'invisibilité numérique se pose…
Sous cette conception, les propriétés du cyberespace, relativement à la question de l'invisibilité, sont doubles. Mémoire et surveillance le caractérisent.

a) La mémoire

La technologie numérique possède sa mémoire propre. A la différence de l'être humain, la machine ne pense pas. Elle exécute. Toutes les traces de ses instructions et exécutions ne constituent donc pas un fonds d'impressions cognitives, mais un simple journal de bord, sans chaleur ni contexte.
Pourquoi cette précision ? Parce que la mémoire humaine repose sur la *sélection*. La fonction d'oubli est capitale pour l'équilibre de la psyché. La mémoire biologique, contrairement à ce que l'on pourrait penser, repose sur l'effacement de l'inutile et la conservation d'une empreinte de ce qui apparaît comme pertinent[16]. A partir de ces empreintes, une image du souvenir pourra être reconstituée *ex post* pour les besoins contemporains de la personne, dans le contexte qui est actuellement le sien. Mais à proprement parler, *la mémoire humaine n'enregistre pas les données brutes du quotidien*, et l'essentiel de son travail consiste à faire le tri. Lorsque cette fonction d'oubli – ou de sélection, selon comment on l'envisage – vient à faire défaut, le sujet souffre alors d'une potentielle *hypermnésie* qui, loin d'être un avantage, va considérable l'affecter psychologiquement dans son développement et sa vie personnelle. L'hypermnésie constitue une pathologie, et non un état normal.
A l'inverse, la mémoire numérique enregistre les signaux tels quels, sans distinction ni perte spontanée. La machine conserve le journal de son activité, écrit en langage numérique, aussi longtemps qu'une instruction d'effacement n'a pas été donnée. C'est là une différence fondamentale avec la société humaine, fondée sur la mémoire biologique et sa transposition sociale qui sélectionne les faits

[16] Voir V. MAYER-SCHÖNBERGER, *Delete : The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2011, pp. 16 s.

pertinents, efface les faits non pertinents, et recontextualise les évènements anciens lorsqu'elle se les remémore. La machine enregistre sans discernement et permet en conséquence une consultation et une analyse sans discernement du passé numérique. Cette propriété de la mémoire numérique engendre une capacité de surveillance tout simplement gigantesque. A partir du moment, en effet, où les machines sont reliées entre elles et où il est possible à distance, d'une machine à l'autre, de consulter au moins une partie de l'historique d'activité de l'autre, tout ce qui est fait dans l'enceinte d'une machine peut potentiellement être connu d'un tiers à l'extérieur. La mise en relation par le cyberespace de l'ensemble des machines permet la consultation potentielle, sous les réserves techniques et juridiques qui s'imposent, d'une mémoire précise, objective et indépendante des évènements ultérieurs. Bien évidemment, la mémoire numérique présente d'immenses avantages, pour la science ou le droit, notamment. Ses fonctions d'archivage ou de preuve en sont un parfait exemple. Mais en ce qui concerne la protection de la vie privée, la mémoire numérique est nettement plus dangereuse pour les personnes : c'est elle qui permet la surveillance de masse.

b) La surveillance

Dès l'instant que l'on envisage la question d'un droit à l'invisibilité numérique, il apparaît indispensable de souligner à quel point le cyberespace expose ses utilisateurs à une forme de surveillance entièrement nouvelle dans l'histoire. D'une ampleur inédite, elle revient à observer une masse de données enregistrées, collectées puis analysées, dont découlent ultérieurement toute sortes de décisions économiques ou politiques.

Sous cet angle, la surveillance numérique peut être définie comme le fait d'accéder en tout ou partie aux données et métadonnées de l'utilisateur d'une machine connectée, dans le but de procéder, après collecte de celles-ci, à des analyses individuelles ou collectives, dont des décisions ultérieures, économiques ou politiques, découleront[17].

Ainsi entendue, elle regroupe aussi bien la collecte de données et métadonnées consentie par l'utilisateur d'un appareil en échange d'une consultation gratuite d'un site, et dont la fonction est d'ouvrir la voie à des analyses commerciales, que celle réalisée par ou pour le compte des États – ou plus largement des personnes publiques – dans le but de se renseigner sur la situation du territoire et le comportement collectif ou individuel de citoyens. Les deux types de surveillance, sous cette perspective, poursuivent des buts

[17] L'essentiel de la surveillance a une fonction politique ou économique. Pour autant la surveillance personnelle existe aussi, si l'on entend par là le fait pour une personne physique d'observer par l'outil numérique une autre personne physique pour un motif personnel. Elle relève alors davantage d'un travail de détective – voire de l'espionnage, si elle s'exerce dans un cadre illégal – qui ne relève du champ d'investigation que circonscrit la discussion sur la reconnaissance d'un éventuel droit à l'invisibilité numérique.

différents et soulèvent des questions distinctes quant à leur légalité ou leur légitimité. Pour la surveillance privée, la question fondamentale est celle de la réalité du consentement de l'utilisateur qui, pour passif qu'il est, n'a généralement pas conscience de l'étendue ni de l'importance des données et métadonnées qui lui sont collectées. Elle est aussi celle du modèle économique que le web a engendré. La gratuité d'accès aux sites se paye en réalité par l'acceptation de la collecte de données, si bien que la data se transforme en une sorte de valeur d'échange. Pour la surveillance publique, elle pose la question de la protection du citoyen contre l'État, puisque ce dernier peut, par ce biais, détenir une forme de puissance qui n'a jamais existé dans l'histoire. Le renseignement général a toujours existé, et il est normal que le Prince cherche à connaître l'état du pays qu'il gouverne. Toutefois, il atteint ici, grâce à une collecte à grande échelle et au calcul par algorithme, une puissance inégalée. Dans les périodes sombres de l'histoire, aucun tyran n'a jamais su, aussi précisément que cela est possible désormais, ce que pensait le peuple dans son ensemble, et ce que pensait un individu isolément. Aujourd'hui, cela serait théoriquement possible si une telle arme tombait entre de mauvaises mains. Les possibilités de répression et de persécution de la population en seraient terrifiantes. Par conséquent, la question de l'invisibilité n'est pas seulement une question de préservation de la personne, prise en elle-même : elle est aussi une question fondamentale de préservation de l'État de droit.

En toutes hypothèses, et indépendamment du but poursuivi, la surveillance est une donnée fondamentale du cyberespace contemporain. Que ce soit par *cookies*, *Java script*, *Ghost Trackers* ou *emails scanning*, toute cyberactivité néophyte est transparente. La moindre utilisation d'un matériel connecté donne lieu à collecte de données ; et ce, ne serait-ce que dans le cadre légal, puisque consenti par l'utilisateur, ainsi que le *Règlement général sur la protection des données* (ci-après RGPD)[18] de l'Union européenne le prévoit. A côté de cela, la surveillance discrète, pour ne pas dire illégale, par les services de renseignement des États existe également. La révélation du programme *PRISM* par Edward Snowden en constitue le parfait exemple. Selon ce dernier, la NSA aurait conçu un système de collecte de l'ensemble des informations circulant par les câbles sous-marins reliant les continents, en vue de leur centralisation et analyse à la demande par ses supercalculateurs. Si cela était parfaitement exact, cela signifierait que les États-Unis pratiqueraient – ou auraient pratiqué – une surveillance de masse de l'ensemble des données de la communication mondiale. Il est difficile de fournir un meilleur exemple en faveur de la légitimité d'un droit à être invisible, dans de telles conditions… Un tel droit ne serait, de ce point de vue, qu'une forme tout à fait logique de légitime défense.

[18] Règlement UE n°679/2016 du 27 avril 2016, JOUE (2016) L 119-1.

Mieux encore, cette surveillance peut potentiellement s'exercer à l'abri des lois nationales. Ainsi, lorsqu'il est question d'analyser les données collectées, le RGPD encadre strictement le type d'analyse qui peut être réalisé à partir des données personnelles afférant au comportement de personnes dans l'Union européenne. Sont ainsi prohibées, en principe, les traitements de données qui révèlent notamment l'origine raciale ou ethnique, les opinions politiques, la religion, la santé, l'orientation sexuelle, ou les données biométriques d'une personne permettant son identification. L'article 9 du règlement l'interdit de façon explicite. Des exceptions sont évidemment prévues, notamment lorsque de tels traitements sont réalisés pour servir un intérêt public, assurer la sauvegarde des intérêts vitaux d'une personne, ou lorsque le consentement spécial de la personne a été recueilli conformément à au droit national. Mais la question qui se pose, dès lors que l'on a à l'esprit les caractères intrinsèquement international et décentralisé du réseau internet, est celle de l'effectivité d'une telle prohibition. En effet, dès l'instant que les données collectées dans l'Union européenne – ou depuis l'extérieur de l'Union européenne par l'emploi d'outil de surveillance à distance – sont transférées vers un État tiers qui n'est pas soumis au RGPD, ou qui, plus malicieusement, s'y soustrait de fait, rien ne semble plus faire obstacle à la réalisation des analyses prohibées puis à leur commercialisation, en tout ou partie, à un client public ou privé les recueillant à l'extérieur de l'Union, pour garantir la discrétion de cette opération, avant d'en faire un usage ciblé et non avoué sur le territoire de celle-ci. Certes, en ce qui concerne les États-Unis, l'adoption du programme *Privacy Shield* garantit le contrôle et la surveillance par l'État fédéral américain du transfert et traitement des données recueillies dans l'Union européenne. Les règles qu'il définit sont conçues pour garantir l'équivalence de la protection des données en vigueur dans l'Union à celle ayant cours en territoire américain. Mais ce programme ne fait pas sur ce point sur l'unanimité, tant il peut être suspecté de ne constituer qu'une façade permettant la poursuite du transfert de données, après l'abandon du programme précédent, le *Safe Harbour*, jugé insuffisant à fonder une décision d'équivalence de la Commission européenne pour permettre *a priori* et de manière générale le transfert de données par la Cour de justice de l'Union européenne dans son célèbre arrêt *Schrems* (2015). Le *Privacy Shield* fait d'ailleurs, à ce titre, d'une contestation en cours, notamment devant le juge européen. La conclusion qui s'en infère, pour l'heure, est simple : il n'est pas possible de garantir au citoyen européen de façon certaine que ses données personnelles ne seront pas utilisées, une fois transférées à l'extérieur de l'Union, pour procéder, sur le sol d'un État tiers, à un traitement qui serait pour sûr illégal fût-il réalisé sur le sol européen. Dans ces conditions, la surveillance du cyberespace ne trouve pas nécessairement de remède absolu dans l'encadrement du traitement des données, car ce qui est réglementé en un lieu peut ne pas l'être en un autre, où il peut être aisé de

transférer les données pour se libérer de la réglementation initialement applicable. L'état de surveillance du cyberespace se distingue par une marqueterie de lois, où le *legal shopping* est d'autant plus aisé qu'il ne requiert pas nécessairement de déplacement physique des personnes. On comprend dans de telles conditions que la visibilité de la vie des personnes n'a jamais été aussi grande dans l'histoire, ni aussi puissante dans ses conséquences économiques et politiques. Or si la *visibilité* s'élève à un tel degré, le remède à ses effets pervers peut tout simplement être, par voie de réciprocité, l'*invisibilité*. Des techniques le permettent déjà, du reste.

2) Les outils de l'invisibilité

Dès l'instant que l'on définit l'invisibilité comme l'occultation d'un état, à un instant précis et sous un angle d'observation déterminée, ainsi que cela a été fait plus haut, la recherche de cette qualité ne relève pas de l'utopie dans le monde numérique. Diverses techniques existent pour cela. Le présent exposé se bornera à n'en exposer que quelques-unes, choisies parmi les principales, selon leur mode d'intervention.

Le premier outil est le *réseau privé virtuel* (VPN). Celui-ci peut être défini comme un système permettant de créer à distance un lien direct entre des ordinateurs, qui isole les échanges d'information du reste du trafic se déroulant sur des réseaux de télécommunication publics. Avec un tel système, deux utilisateurs peuvent converser à distance à travers le réseau internet sans passer par des intermédiaires, et notamment sans que le fournisseur d'accès (FAI) ne puisse consulter les données. En temps normal, toutes les communications transitent par le FAI. Ce dernier constitue un intermédiaire amené à détenir, par conséquent, les données et métadonnées de ses clients. Le VPN crée, nonobstant l'intrication des échanges conduits sur internet, un réseau local auquel n'ont accès que les utilisateurs agréés. Il peut se doubler, par sécurité, d'un dispositif de cryptographie, de manière à rendre les échanges impénétrables à celui qui réussirait, malgré tout, à les intercepter. Ainsi entendu, le VPN permet de dissimuler à toute personne non agréée les communications des utilisateurs. Il opacifie leur contenu, *a fortiori* par le recours adventice à la cryptographie, et crée artificiellement un réseau local d'échange de données. Sa principale fonction est donc de rendre invisible le contenu et la signification des communications menées sous sa protection. Il peut masquer la localisation de l'utilisateur, en lui conférant une adresse IP apparente distincte de son adresse réelle, et rendre sa position et son identité invisibles. Pour accroître cette protection, le recours à un VPN sans registre d'activité, dit *VPN No Log*, s'avère indiqué. En effet, dès l'instant qu'un VPN ordinaire est utilisé, le FAI ne dispose plus d'informations sur l'activité des ordinateurs utilisés. C'est l'opérateur offrant un service de VPN qui centralise lesdites informations. Ces dernières ne transitent plus

que par lui. En théorie, le prestataire de service qui prodigue le VPN peut donc, en lieu et place du FAI, recueillir lui-même les données et métadonnées. En ce qui concerne les métadonnées, il peut ainsi enregistrer l'adresse IP entrante et sortante, l'horodatage des connexions et la quantité de données transférées. Et en ce qui concerne les données, il peut consigner la liste des sites visités, les fichiers téléchargés et le logiciel employé par l'utilisateur. Autrement dit, la surveillance passe des mains du fournisseur d'accès à celles du prestataire de service VPN. Si ce dernier est situé dans l'Union européenne, il peut être tenu par la loi de l'État membre de son établissement de conserver certaines données et métadonnées pour les communiquer au besoin aux autorités administratives ou judiciaires dudit État, notamment lorsque l'intérêt public est en jeu[19]. Un VPN No Log est précisément conçu pour s'affranchir de cet état de fait. Il se distingue en effet par l'omission de tenue de tout registre d'activité, que ce soit pour les données ou les métadonnées, d'une part ; et, d'autre part, par l'établissement de l'entreprise qui l'exploite dans un État tiers à l'Union européenne, et en dehors de surcroît des États-Unis. Ceci, pour échapper à l'application du droit européen et du droit américain. La confiance qui peut être accordée à un tel service dépend de celle que l'utilisateur est prêt à consentir, notamment sur la foi des auditeurs indépendants amenés à contrôler, à titre purement privé et commercial, que ledit prestataire respecte bien les obligations d'omission de registre et de localisation exclusive hors l'UE et le territoire américain. Comme parfois dans le monde numérique, la confiance d'entreprise remplace le contrôle régalien. Avec un tel outil, il est possible de communiquer à distance sans laisser le FAI collecter et enregistrer les données échangées, rendant ainsi le contenu du dialogue invisible à ses yeux. Il y a là invisibilité partielle du discours par escamotage de l'intermédiaire ordinaire.

Le second outil qui vient à l'esprit est le réseau *Tor,* lequel peut être défini comme un réseau alternatif superposé au réseau internet dont la conception permet de garantir l'anonymat des utilisateurs, d'une part, et la consultation de sites exclusivement accessibles par lui, d'autre part. Issu des travaux de l'armée américaine, et bâti à l'origine pour garantir la discrétion des échanges de données à caractère militaire, le réseau Tor est aujourd'hui accessible à tous, sans que son usage basique ne requiert de compétences avancées en informatique. Par son biais, il devient possible à l'utilisateur du navigateur dédié – le *Tor Browser* – qui use par ailleurs d'un *VPN No Log* de consulter tous les sites internet ordinaires, sans trahir son identité. Il peut également être accédé à l'ensemble du *deep web*, c'est-à-dire des sites en *.onion*, dont la consultation est impossible sans recours au *Tor Browser*. Ces sites permettent la consultation, la

[19] Voir ainsi en France les dispositions de l'article L 34-1 du Code des postes et des communications électroniques.

publication ou l'échange d'information dans le plus parfait anonymat, puisqu'il est techniquement difficile, sinon impossible, d'identifier les personnes, toutes dissimulées derrière les fausses adresses IP fournies par le navigateur. Il se crée à travers lui un espace de discussion où règne l'invisibilité d'identité et de localisation. Le recours à la cryptomonnaie, pour prohiber toute traçabilité en évitant le secteur bancaire réglementé, parachève le système en ouvrant la voie à la réalisation de transactions financières intraçables. C'est ce qui a permis à Tor d'abriter un versant obscur, dit *Dark Web*, où prolifèrent les sites illégaux, offrant à la vente de la drogue, des armes, des faux papiers et toutes sortes de marchandises illicites, ou proposant des services criminels telle que la consultation de pornographie illégale, c'est-à-dire composée de scènes de viol, de torture ou de pédophilie. Il est difficile de quantifier avec exactitude la part sombre de ce royaume de l'invisibilité numérique. Des estimations ont cependant pu être réalisées. Selon une étude réalisée en 2016 sur un panel de 5205 sites, 1547 d'entre eux proposaient effectivement des marchandises ou des services illégaux[20]. Si l'on consent à généraliser le résultat, il en ressortirait que le *Deep web* serait composé à environ 30% de services criminels. C'est évidemment beaucoup. La proportion est sans doute très supérieure au ratio de criminalité du web classique. Mais la discrétion que Tor prodigue permet aussi aux dissidents politiques des régimes dictatoriaux de s'exprimer et de communiquer à l'extérieur, aux journalistes de contacter leurs sources sans risquer de les compromettre[21], et plus largement à tout citoyen d'explorer un territoire où règne une parfaite liberté d'expression, puisque le contrôle étatique ne peut s'y exercer. Tor est à la fois un outil de démocratie, de liberté et de crime par-delà les frontières[22].

Un troisième instrument d'invisibilité numérique peut être regardé dans les réseaux informatiques alternatifs, qui, nonobstant leur différence de fonctionnement technique, permettent également d'échanger des informations en toute discrétion. Les réseaux *Freenet, I2P* ou *Zeronet* en constituent de parfaits exemples. *Freenet* est ainsi un réseau anonyme permettant la consultation de sites, la fourniture de services de messageries et le stockage chiffré d'informations. *I2P*, de façon différente, garantit sur le réseau dédié l'anonymat de l'utilisateur par la substitution d'une clé cryptographique à l'adresse IP classique, de manière à rendre l'identification impossible au cours du décryptage. *Zeronet*, enfin, se constitue d'un réseau informatique de pair à pair, dans lequel les informations sont stockées en mode crypté par les utilisateurs eux-mêmes, de façon à ce que ces derniers puissent échanger directement à partir de la plate-forme qui les met en relation – à

[20] D. MOORE, T. RID, "Cryptopolitik and the Darknet", *Survival*, 2016, 58:1, pp. 7-38.
[21] K. D. WATSON, "The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks", *Washington University Global Studies Law Review*, nº 11, 2012, p. 718.

l'instar d'un courtier informatique – sans passer par des intermédiaires qui conserveraient potentiellement les données. Adjointe au navigateur Tor, le recours à *Zeronet* permet de rester invisible à la censure et d'échapper pour l'essentiel à la surveillance. Un quatrième outil d'invisibilité ressort, pour ce qui a trait à la couche physique au sens défini plus haut, du système d'exploitation amnésique *Tails*. En temps ordinaire, et sauf usage d'un tel système d'exploitation, un ordinateur conserve des traces de son activité sur le disque dur. Autrement dit, il peut être comparé de ce point de vue à un navire dont le capitaine consigne chaque jour les évènements survenus à bord. La saisie matérielle de l'ordinateur et l'extraction du disque dur permet par conséquent de consulter cette activité et ainsi de trahir les actions de l'utilisateur. La recherche d'une invisibilité totale passant par l'effacement de toute trace et mémoire, un système comme *Tails* s'illustre tout particulièrement à cet égard. Conçu pour fonctionner en mémoire morte, c'est-à-dire sans persistance de l'information après extinction de l'appareil, il ne laisse aucune trace. Lorsque l'ordinateur est éteint, toute trace disparaît. Même si l'ordinateur était physiquement capturé par un attaquant, son analyse ne révèlerait rien de l'usage qui en a été fait, car sa mémoire serait vide.

Enfin, un cinquième outil ressort en la matière de l'usage de la cryptomonnaie. Celle-ci, en tant qu'unité de valeur consentie conventionnellement par ses utilisateurs pour leurs échanges réciproques, consignée par un registre et garantissant par la cryptographie l'anonymat de l'utilisateur, constitue l'instrument des échanges anonymes entre sujets désireux d'éviter l'identification, la traçabilité et le contrôle prudentiel et réglementaire que garantit le système bancaire classique. Le *Monero*, par exemple, constitue une forme de cryptomonnaie particulièrement protectrice de l'invisibilité, puisque sa structure est conçue pour empêcher le traçage de l'émetteur du paiement, du montant de la transaction, et de la destination des fonds. Il est alors possible de « payer » sans qu'il soit possible de savoir qui paye qui et pour quel montant.

Le recours à l'ensemble de ses techniques permet à l'utilisateur averti de consulter, d'échanger et de publier des informations en échappant à la surveillance et l'identification personnelle. Une fois invisible au sens défini plus haut, l'utilisateur peut en profiter pour contourner la censure d'un régime politique dictatorial, informer le public d'un scandale, ou tout simplement protéger sa propre vie privée parce qu'il en a le loisir. Il peut aussi s'en servir pour accéder à du contenu illégal et commettre lui-même des crimes et délits. La question se pose alors de savoir s'il convient de reconnaître en tant que tel un *droit à l'invisibilité*, ou si, au contraire, cet état d'invisibilité ne saurait constituer une prérogative reconnue du sujet de droit.

§ 2 – Y-A-T-IL UN DROIT À L'INVISIBILITÉ NUMÉRIQUE ?

A ce jour, l'invisibilité a presque toujours été regardée comme un mythe, et non comme un état dont l'usage constituerait une prérogative de la personne. Ainsi, elle a pu être considérée à travers des manifestations partielles, telles que celles de l'anonymat ou de la dissimulation de l'adresse IP.

Rien n'interdit pour autant de poser la question d'un droit fondamental à l'invisibilité sous une perspective générale. L'intérêt d'une telle démarche est triple. Tout d'abord, elle permet d'unifier le débat autour des différentes formes de la discrétion numérique. De la réponse qu'elle appelle, les analyses adventices de l'ensemble des techniques de dissimulation dépendront. Ensuite, une telle généralité d'appréhension a pour vertu de couvrir l'émergence prévisible de futures techniques de furtivité, dans un domaine où, précisément, les inventions sont souvent en avance sur les analyses juridiques qu'elles appellent. Plus la question est posée à un niveau élevé d'abstraction théorique, plus elle est de nature à englober d'éventuelles variétés nouvelles de l'invisibilité numériques. Identifier le genre, de ce point de vue, facilite la compréhension de l'espèce. Enfin, le choix de cette échelle de réflexion se justifie par l'éclairage qu'il est susceptible d'apporter sur la coexistence des droits et libertés fondamentales, dont l'invisibilité serait, ou ne serait pas, le perturbateur.

Si l'on retient cette perspective, la question fondamentale serait la suivante : *Puisque le citoyen n'a jamais été autant vu qu'aujourd'hui lorsqu'il use des outils numériques, ne faudrait-il pas tout simplement protéger celui par la reconnaissance d'un droit à ne pas être vu, c'est-à-dire d'un droit à l'invisibilité ?*

Pour trancher cette question, l'examen de ses termes exacts s'impose, avant que toute proposition de solution ne soit émise.

A) Examen du problème

Le débat fondamental procède de la réaction à la surveillance, et de l'instinct naturel de préservation de la vie privée, lorsque, puissamment attaquée, celle-ci requiert une protection d'égale puissance.

Mais une suggestion naturelle ne résiste pas, en toutes choses, à l'examen approfondi. C'est pourquoi l'examen des arguments en faveur de l'une et l'autre thèse, celle de la reconnaissance d'un tel droit à l'invisibilité, et celle du rejet d'une telle reconnaissance, s'impose.

1) Les arguments pro

Quatre arguments plaident selon nous de façon sérieuse en faveur de la reconnaissance d'un droit à l'invisibilité. Aucun ne limiterait pour autant les possibilités d'encadrement, de contrôle ou de

limitation d'un tel droit, viendrait-il à être reconnu. Mais ils en assoiraient la légitimité.

Le premier argument *pro* réside dans la puissance d'intrusion de la surveillance numérique. Comme il a été dit plus haut, et ainsi que cela se reconnaît largement, l'utilisateur des nouvelles technologies, cet *Homo numericus,* a troqué, souvent sans le savoir, sa vie privée, et plus spécifiquement ses données personnelles, en échange d'un usage facilité ou gratuit des outils numériques. Le citoyen n'a jamais été autant vu, que ce soit par les entreprises commerciales – dont le modèle économique se fonde sur la collecte et l'analyse de data – ou que ce soit par les États. Or il ne sert à rien de maintenir une protection classique de la vie privée, issue des article 8 de la Convention européenne des droits de l'homme et 7 de la Charte des droits fondamentaux de l'Union européenne, ou, en France, de l'article 9 du Code civil, si cette protection est réduite à peau de chagrin par le rapetissement de son champ réel de protection, du fait de la prépondérance désormais irréversible de l'outil numérique. La vie privée, et même la protection des données personnelles, ont été à l'origine conçues à une époque où l'information circulait par des canaux *analogiques*[23], tels que le journal papier, la télévision cathodique, la correspondance postale, ou les ondes radio. Par ailleurs, la plupart des outils de lecture de l'information reposaient eux-mêmes sur l'interprétation sonore ou visuelle de l'empreinte analogique laissée par le signal initial que constituaient le son d'un instrument, d'une voix, ou, différemment, la lumière impressionnant une pellicule argentique. Ces outils n'étant ni connectés entre eux, ni reliés à un fournisseur d'accès, ils ne collectaient ni n'enregistraient aucune donnée ni métadonnée. Il n'en va pas de même aujourd'hui, ou plus de 98% de l'information circule sous un format numérique. Les techniques de communication et de diffusion de l'information face auxquelles la vie privée classique s'est affirmée ne sont plus employées que pour 2% au mieux de l'information que nous émettons et recevons. Il peut donc être considéré que la vie privée et la protection des données personnelles classiques, issues du monde analogique, ont été littéralement phagocytées par la technologie numérique. Certes, il pourrait être opposé que ce phagocytage a été, et reste encore largement, consenti quotidiennement par les personnes ; ce dont il découlerait qu'il n'y aurait là aucune véritable *intrusion* dans la vie privée. Là où la personne consent, il n'y a pas d'intrusion ; et ce, pas plus qu'il n'y a d'effraction lorsque l'on accepte de son plein gré la présence de quelqu'un chez soi. Mais ce n'est là qu'une vue de l'esprit, en vérité. Rares sont en effet les utilisateurs qui ont véritablement conscience de ce à quoi ils consentent en utilisant leurs outils numériques connectés ; outre que, de surcroît, la pression sociale et professionnelle les contraint quoiqu'il en soit à utiliser ces outils, qu'ils le veuillent ou non. Une image assez simple

[23] *Interview with Viktor Mayer-Schoënberger, op. cit.* n.3, p. 326

permet de s'en persuader. Aucun citoyen n'accepterait par exemple, dans le monde réel, de lire tranquillement un journal devant la cheminée, tout en étant observé à la loupe dans chacun de ses gestes de lecture par une quinzaine d'employés de sociétés commerciales faisant irruption dans la pièce, en échange de la gratuité du journal… Or c'est pourtant ce qui se produit lorsque l'on consulte, sans précaution particulière, le site internet du même journal, à travers l'ensemble des programmes fantômes qui collectent les données de l'utilisateur. Si cela se produit donc *mutatis mutandis* pour la lecture d'un journal numérique, cela ne pourrait être que parce que le citoyen est *berné* par la technologie numérique, dont il ne perçoit pas les propriétés de surveillance.

Le second argument *pro* réside, face à cette intrusion de masse, dans l'égalité des citoyens. Le principe d'égalité de droit est une composante essentielle de la vie démocratique moderne. La *Déclaration universelle des droits de l'homme* (1948) l'érige en principe fondamental dans son article 1er. La Charte des droits fondamentaux de l'Union européenne l'énonce quant à elle dans son article 20. La Convention européenne des droits de l'homme le formule à travers l'interdiction des discriminations qu'elle énonce à l'article 14. En droit français, le principe d'égalité entre les citoyens occupe une place de premier rang dans la Constitution, qui l'énonce dans son article 1er. Or, l'intrusion technologique dans la vie privée des personnes, par leur consentement passif pour l'essentiel non éclairé, d'une part, et par la surveillance indépendante de leur volonté, d'autre part, diviserait les citoyens en deux catégories. La première catégorie se constituerait des personnes qui n'ont pas conscience de la surveillance et l'observation dont elles sont l'objet, c'est-à-dire l'immense majorité de la population ; ainsi que de celles qui, bien qu'ayant une certaine connaissance voire conscience de la profondeur de l'intrusion, ne disposeraient nullement des connaissances et moyens techniques permettant, par des outils de discrétion numérique, de protéger leur sphère personnelle en se rendant, en tout ou partie, invisibles. A l'inverse, la seconde catégorie, très largement résiduelle, se composerait des initiés, capables d'employer, en toute sécurité numérique, c'est-à-dire sans commettre de fautes, les outils de discrétion dédiés, tels que la cryptographie, les réseaux alternatifs et les systèmes amnésiques. Cette division de la population citoyenne en deux catégories aurait pour conséquence d'introduire une inégalité dans l'exercice effectif du droit de chacun à protéger sa vie privée et ses données personnelles. Les experts en informatique pourraient se protéger de l'intrusion en se rendant, en tout ou partie, invisibles, tandis que les néophytes, par la force des choses, en resteraient incapables. Certes, cette inégalité ne serait *a priori* qu'une inégalité de fait, et non une inégalité de droit. A ce titre, elle ne justifierait pas nécessairement une résorption radicale par la reconnaissance d'un droit fondamental nouveau. Mais il pourrait être opposé à une telle objection que lorsque l'inégalité de

fait ne profite qu'à une infime partie de la population et prive pour une très large part l'immense majorité de la population d'une mise en œuvre effective de son droit à protéger sa sphère personnelle, le hiatus entre le fait et le droit devient tel qu'il dévitalise purement et simplement la vie privée. Or l'art du droit reste celui de rendre à chacun son dû, et non pas celui de proclamer des idéaux théoriques dont la mise en œuvre réelle confine à l'illusion. Prise sous cette perspective, l'effectivité du principe d'égalité commanderait de reconnaître à chacun le droit d'être invisible en tout ou partie dans la sphère numérique ; ce dont découlerait alors l'obligation positive des États de faire en sorte que des outils simples et accessibles soient mis à la disposition de chacun à cette fin.

Le troisième argument *pro* surgit du caractère intrinsèquement innovant qui distingue le droit du numérique. Cet argument présente pour l'essentiel un caractère réplicatif, car il consiste à réfuter l'obstacle qui vient immédiatement à l'esprit, et qui suggère qu'il serait tout simplement impossible de reconnaître un droit à l'invisibilité, puisqu'un tel droit – sauf erreur de notre part – n'a jamais existé dans l'histoire. Il réfuterait aussi l'opposition technique que ne manqueraient pas de formuler ceux qu'un tel droit perturberait dans leur pratique ou leur modèle économique. La réponse serait simple, sous cet angle. S'il n'a jamais existé de droit à l'invisibilité, c'est parce que la visibilité n'avait jamais atteint auparavant un tel seuil. En instituer un aujourd'hui serait certes une innovation, mais ladite innovation interviendrait dans un contexte qui ne peut être comparé avec celui du passé. Par ailleurs, l'histoire a montré que l'on a pu créer un droit à l'oubli numérique, bien qu'il ait été régulièrement opposé par les détracteurs d'un tel droit que cela fût techniquement impossible. La Cour de justice a reconnu le droit à l'oubli numérique dans son arrêt *Google Spain* (2014), avant que l'article 17 du RGPD ne le consacre en droit écrit ; et les géants du numérique s'y sont adaptés *volens nolens*. Preuve, s'il en est, que l'argument de l'impossibilité technique prétendue est parfois à relativiser.

Enfin, le quatrième argument s'infère, par réfutation, des conséquences qu'engendrerait un refus persistant de reconnaître tout droit à l'invisibilité dans le monde numérique. Alors qu'il est naturel de fermer portes et fenêtres à domicile, lorsqu'on désire être invisible au regard extérieur, il n'existerait aucun droit à le faire dans le monde numérique. Ce dernier serait condamné à devenir un gigantesque *Panoptique*, à l'usage indispensable dans la vie personnelle et professionnelle, mais où il serait impérieux de payer son écot en acceptant la surveillance de nos moindres faits et gestes. Cette curieuse perspective démontrerait, à l'évidence, que l'invisibilité physique, totale ou partielle, étant déjà reconnue, il conviendrait d'en transposer l'usage et la reconnaissance par l'admission d'un droit fondamental spécifique.

Ces arguments sont, on le voit, sérieux. Ils peuvent toutefois rencontrer une solide contradiction.

2) Les arguments contra

Le premier obstacle s'opposant à la reconnaissance d'un quelconque droit à l'invisibilité peut être qualifié d'*argument de police*. Chacun sait que la vie en société n'est possible que si une force légitime, organisée et efficace, garantit le respect de la loi par les citoyens, au besoin par le recours à la contrainte. S'il n'est pas de liberté sans loi, il n'est pas davantage de société sans police. La forme et les moyens de la fonction de police peuvent varier avec le temps et les cultures. Mais l'autorité politique ne peut jamais se dispenser de police, sauf à disparaître. Pour reprendre l'expression célèbre de Max Weber, l'État détient le « *monopole de la violence légitime* ». Or, à l'évidence, il serait absurde de reconnaître aux citoyens, dans la sphère numérique, le droit d'échapper à toute surveillance. Cela reviendrait, ni plus, ni moins, qu'à bander les yeux de la police. Imaginerait-on une société où les policiers porteraient un bandeau sur les yeux pour ne pas voir les citoyens qu'ils protègent et ceux qu'ils surveillent, voire interceptent ? Une telle idée relèverait du théâtre de l'absurde. Si la surveillance fait problème, c'est par son contenu et ses modalités. Ces dernières peuvent être débattues démocratiquement. Mais pas la surveillance dans son principe même, sauf à souhaiter une forme d'anarchie. La police – dont la surveillance est l'une des missions – ne fait que traduire naturellement l'*imperium* de l'autorité politique. Il serait donc inconcevable, de ce point de vue, de reconnaître de façon générale un droit à l'invisibilité, puisque cela reviendrait à amputer la société politique d'une de ses composantes vitales.

Le second argument *contra* procède de la *clarté du droit*. En effet, dans un système juridique sain, ou bien un fait relève de prescriptions normatives, et dans cas il est réglementé ; ou bien, au contraire, il n'en relève pas. Ainsi, si l'on considère l'ordre juridique étatique, il n'est pas permis de proférer publiquement de accusations fausses et précises à l'encontre d'autrui, sous peine de commettre une diffamation. En revanche, à domicile, et dans le cercle privé, rien n'interdit de faire de même pour laisser libre cours à une hostilité personnelle. Si la morale en pâtit, le droit en sort indemne. La différence entre ces deux situations réside fondamentalement dans le *périmètre* de l'interdiction de la diffamation. Celle-ci ne concerne que les propos publics, à l'exclusion des propos privés. Dès lors, de deux choses l'une. Ou bien la situation tombe dans le champ de la norme, et dans ce cas celle-ci doit s'appliquer effectivement ; ou bien, au contraire, ce n'est pas le cas, et dans ce cas elle ne s'applique tout simplement pas. Mais il ne doit pas y avoir de situations intermédiaires ou mixtes, dans lesquelles la norme est applicable en tout ou partie, tandis que la personne peut trouver à s'en soustraire aisément. Pour le dire autrement, l'eau doit être claire ou opaque. Or une bonne législation ne doit pas s'accommoder d'*eaux troubles*. Si l'on suit ce raisonnement, il y a lieu de rejeter l'idée d'un droit à l'invisibilité. Sa

reconnaissance reviendrait à créer partout, chaque fois qu'il est employé, de véritables eaux troubles. En effet, il serait par exemple interdit à tous de se livrer à du trafic de stupéfiants, mais il serait légal à chacun d'user des technologies nécessaires à l'exercice en toute discrétion de celui-ci sans que cet usage criminel ne puisse en soi être remis en cause. L'absurdité d'une telle situation serait patente, et commanderait de récuser toute reconnaissance possible d'un droit à l'invisibilité.

Le troisième argument *contra* s'infère de *l'absence de hiérarchie entre les droits fondamentaux*. D'une manière générale, il est admis que le droit à la vie chapeaute tous les autres droits. La raison à cela est la fois éthique et chronologique. Sauf à emprunter une voie funeste, la morale ne saurait admettre qu'un système juridique ait pour objet de porter atteinte à la vie. Même la force – y compris dans la forme potentiellement létale qu'elle peut emprunter, spécialement lorsqu'elle s'exprime par la guerre – ne peut être employée que pour défendre, précisément, la vie des citoyens et le maintien des règles qui la protègent. Par ailleurs, sur le plan chronologique, la vie du sujet de droit préexiste nécessairement au droit lui-même. Tant qu'il n'y a pas de sujet, il n'y a pas de droit. Pas de droit sans personne, pas de droit sans vie, pourrait-on dire. C'est pourquoi le droit à la vie fonde tous les autres[24]. Néanmoins, mis à part le droit à la vie, l'on peut sérieusement douter qu'il puisse exister une quelconque hiérarchie entre les droits fondamentaux[25]. En droit international, la résolution de 1977 de l'Assemblée générale des Nations-Unies proclame l'indivisibilité des droits fondamentaux, et la Déclaration de Vienne du 25 juin 1993 en réitère l'expression[26]. Certes, il est des principes sous-tendus par les droits de l'homme qui méritent une protection particulièrement stricte, eu égard à la gravité que leur violation peut représenter pour la vie démocratique. Tel est le cas de l'interdiction de la torture, de l'esclavage, ou de la non-rétroactivité de loi pénale[27]. Mais mis à part cette impérativité renforcée, l'opinion majoritaire conclut à l'absence de hiérarchie[28], ou à tout le moins, à la difficulté d'en

---

[24] Ch. QUEZEL-AMBRUNAZ, V. RIVOLLIER, « Une hiérarchie entre droits fondamentaux ? Le point de vue du droit civil », *Revue des droits et libertés fondamentaux (RDLF),* 2019 chron. n°45.

[25] K. TERAYA, "Emerging Hierarchy in International Human Rights and Beyond: From the Perspective of Non-derogable Rights", *European Journal of International Law (EJIL)*, 2001, vol. 12, p. 917.

[26] A. SANGIOVANNI, *Fundamental Rights, Indivisibility and Hierarchy Among Human Rights*, *in: Humanity Without Dignity: Moral Equality, Respect, and Human Rights*, Harvard University Press, 2017. p. 235.

[27] L. HENNEBEL, « Typologies et hiérarchie(s) des droits de l'Homme », *Annuaire international de justice constitutionnelle*, 26, 2011. Constitutions et droit pénal - Hiérarchie(s) et droits fondamentaux. pp. 423-435.

[28] M. AFROUKH, « Une hiérarchie entre droits fondamentaux ? Le point de vue du droit européen », *RDLF,* 2019 chron. n° 43 ; J. D. MONTGOMERY, "Is there a hierarchy of human rights?", *Journal of Human Rights*, 2002, Vol. 1, n° 3, p. 373 ; E. KLEIN, "Establishing a Hierarchy of Human Rights : Ideal Solution or Fallacy ?", *Israel Law Review*, 2008, Vol. 41, n° 3, p. 477 ; A. TAHVANAINEN, "Hierarchy of Norms in International and Human Rights Law", 24 *Nordisk Tidskriftor Menneskerettigheter*, 2006, p. 191.

discerner une de façon précise[29]. L'idée d'une hiérarchie n'est pas pour autant inexistante dans le débat académique. Soutenue par certains auteurs, elle conduit alors à ordonner les droits selon leur efficacité à maintenir en place la classe dominante dans une perspective marxiste[30], ou à distinguer les droits selon qu'ils sont ou ne sont pas susceptibles de renonciation par leur titulaire[31]. Toutefois, une telle hiérarchie ne serait alors qu'implicite[32], puisque les instruments internationaux et nationaux énonçant les droits fondamentaux n'y font pas référence. Au sein du Conseil de l'Europe, la Cour européenne des droits de l'homme considère quant à elle, dans son arrêt *Stec c/ Royaume Uni* (2005)[33], que « *la Convention doit se lire comme un tout et s'interpréter de manière à promouvoir sa cohérence interne et l'harmonie entre ses diverses dispositions* ». Droit à la vie excepté, elle semble manifestement réticente à admettre une hiérarchie des droits fondamentaux[34]. Si l'on retient cette thèse, alors il en découle que ni la vie privée ni le respect des données personnelles ne sont au-dessus des autres droits. *La* Privacy *n'est pas la Reine des droits*. Or, si un droit à l'invisibilité était reconnu, chacun pourrait en faire usage dans son intérêt personnel propre, puisqu'il échapperait dans l'exercice de celui-ci à la surveillance, c'est-à-dire à la police considérée en tant que fonction de maintien de l'ordre en société. Certains en viendraient nécessairement à commettre des crimes et délits, et donc à porter atteinte aux droits des autres citoyens. De ce point de vue, le droit à l'invisibilité deviendrait l'instrument, au nom de la *Privacy*, de l'affaiblissement de tous les autres droits, ou presque. La vie privée et la protection des données se constitueraient en droits supérieurs, imposant leur ascendant hiérarchique à tous les autres. Or, c'est précisément inconcevable dès l'instant que l'on réfute l'idée de toute hiérarchie entre les droits fondamentaux. Un tel droit à l'invisibilité ne saurait par conséquent être reconnu.

Enfin, un quatrième argument *contra* s'infère de ce que l'on pourrait appeler le *principe du traitement à la source*. Lorsqu'un problème survient, il est préférable de le traiter dans ses causes et manifestations, de manière à le faire disparaître. Il est moins raisonnable de le laisser prospérer, quitte à ce qu'il prenne une ampleur considérable, pour ensuite proposer une véritable révolution, en la présentant comme seule apte à traiter les

---

[29] Th. MERON, *On a Hierarchy of International Human Rights*, American Journal of International Law, 1986, Vol. 80, n° 1, p. 1.

[30] C. BROCKETT, *A Hierarchy of Human Rights*, Annual Meeting of the American Political Science Association, New-York, ERIC, 1978.

[31] L-Ph. LAMPRON & E. BROUILLET, « Le principe de non-hiérarchie entre droits et libertés fondamentaux : l'inaccessible étoile ? », *Revue générale du droit*, 2011, 41 (1), pp. 93-141.

[32] F. SUAREZ-MULLER, "The Hierarchy of Human Rights and the Transcendental System of Right", *Human Rights Review*, 2019, vol. 20, pp. 47–66.

[33] CEDH *Stec et al c/ Royaume-Uni*, 6 juin 2005, n° 65731/01 et 65900/01, § 48.

[34] Dans une opinion dissidente exprimée dans l'arrêt *Sahin c/ Turquie* (2018), le juge Ergül affirme quant à lui qu'« *on ne doit pas accepter de hiérarchisation juridique entre les droits de l'homme* ».

conséquences induites par la non-résolution du problème. L'art du droit s'élève à prévenir les conflits, plutôt qu'à les susciter, aiguiser ou multiplier. En droit, comme en médecine, la prophylaxie est une vertu. En conséquence, si le problème provient de la surveillance de masse, et de ce que les citoyens n'ont jamais été autant vus qu'ils ne le sont aujourd'hui, il serait sans doute plus sage de réglementer davantage la surveillance pour protéger les personnes, que de créer un droit nouveau dont l'exercice pourrait engendrer de nouvelles difficultés et bouleverser l'équilibre du système juridique[35].

Les deux thèses, on le voit, se nourrissent d'arguments pertinents mettant chacun en évidence une facette de la réalité. La résolution du problème ne passe pas, dès lors, par la récusation complète de l'une d'entre elles, mais par leur articulation. Telle est la solution qui, selon nous, mérite d'être proposée.

B) Proposition de solution

Pour résoudre le conflit entre la protection du citoyen contre la surveillance numérique de masse et la nécessaire transparence que requiert la fonction de police dans une société démocratique, il nous paraît préférable de reconsidérer l'invisibilité à travers un prisme différent.

Il apparaît approprié, de notre point de vue, de considérer l'invisibilité comme un *fait*, et non comme un *droit*. Lorsque la personne invisible est en tout ou partie dans la sphère numérique, ne laissant que peu ou pas de traces de son action, son état de discrétion numérique ne doit pas procéder d'un droit à l'invisibilité en tant que tel. Il ne constitue qu'un état de la personne. Cet état doit s'apprécier, en tant que simple fait, au regard du régime juridique qui préside à son accès et à son usage. Autrement dit, l'invisibilité constitue la conséquence de l'exercice d'un droit préexistant, et non pas une prérogative autonome de l'individu qui devrait être appréciée en soi.

Si l'on suit cette analyse, alors le régime juridique de l'invisibilité ne requiert aucune invention nouvelle, et en tous cas pas celle de la reconnaissance d'un hypothétique droit spécifique. Il suffit pour identifier son régime juridique de confronter les faits découlant de son usage aux normes pertinentes qui le régissent. En un sens, la maxime du droit romain *Da mihi factum dabo tibi jus* n'a rien perdu de son actualité, puisqu'elle éclairer ici le régime juridique de la discrétion numérique.

[35] Il s'agirait, par exemple, de s'inspirer de la solution de la Cour européenne des droits de l'homme selon laquelle la surveillance des communications du salarié par l'employeur doit nécessairement présenter un caractère proportionné, ainsi que cela ressort de son arrêt *Barbulescu c/Roumanie* du 5 septembre 2017 (n°61496/08, spéc. § 121) ; et ce, en soumettant l'ensemble des collectes et analyses de données, non seulement au consentement de la personne, comme c'est déjà le cas, mais aussi à une justification tirée de la proportionnalité de celles-ci aux droits en présence.

Pour le dire autrement, *l'invisibilité est régie par la loi applicable au droit préexistant qui lui a donné naissance*. Ainsi, la discrétion numérique peut découler tout aussi bien de l'inviolabilité du domicile, que du droit au respect de la vie privée, du droit de propriété, de la liberté d'expression, de la liberté contractuelle, du secret de la correspondance, du régime de la cryptographie, du secret professionnel ou des droits de la défense.

A chaque fois qu'un outil de discrétion numérique est employé, c'est le cadre dans lequel il intervient qui déterminera la loi qui lui est applicable en droit international privé, et le contenu de cette dernière en droit interne.

Quelques exemples permettent de se convaincre de la pertinence de cette analyse.

Considérons tout d'abord le cas de la protection du domicile. En droit international privé, l'inviolabilité du domicile est *a priori* régie par la loi du pays de localisation de celui-ci[36]. En conséquence, si une personne souhaite protéger les données de son domicile en rendant opaques ou intraçables l'activité des appareils connectés qui s'y trouvent, le choix de les faire échapper à la surveillance, notamment à la collecte de données par les échanges dits *M2M – ie* « *machine to machine* » - entre les appareils eux-mêmes, relève de la loi du pays de situation du domicile. Cette dernière définira alors dans quelle mesure il est loisible à la personne d'opacifier son domicile. Cela permet ainsi de pallier la lacune relative dans la protection des données qui découle de l'incertitude du régime de protection des échanges de données entre machines elles-mêmes[37], au moins pour celles relevant du domicile privé. Il en va de même du recours par la personne à un VPN, à son domicile, pour des besoins étrangers à son activité professionnelle. Il relève de la loi du lieu de situation du domicile, sans préjudice d'une éventuelle loi de police, au sens du droit international privé, qui en réglementerait spécialement l'usage.

Considérons ensuite le cas du recours à titre non professionnel à des services de messagerie anonymes et temporaires, que ce soit sur le réseau internet, ou sur un réseau alternatif, comme par exemple *Zeronet*. Ce type d'outil relève du secret de la correspondance. L'utilisateur ne recourt pas à un écrit manuscrit,

---

[36] En droit international privé, la responsabilité civile de l'auteur d'une violation de domicile ne relève pas du champ d'application du règlement UE n°864/2007 du 11 juillet 2007 dit *Rome II* sur les conflits de lois en matière extracontractuelle, puisque les atteintes à la vie privé sont exclues de son champ d'application (art 1.2 g). Chaque État membre applique donc son propre système pour identifier la loi applicable. Mais il y a convergence, en droit comparé, à désigner pour compétente la loi du lieu du délit (*lex loci delicti*), c'est-à-dire par hypothèse la loi du lieu de situation du domicile. Mais en amont, puisque la violation du domicile est une infraction pénale, il y a lieu de considérer que l'inviolabilité du domicile en soi, indépendamment de la responsabilité civile des atteintes qui lui sont portées, s'impose par nature de façon territoriale, si bien qu'elle devrait *a priori* relever de la loi du lieu de sa situation, et non pas de la loi applicable au statut personnel de l'individu.

[37] S. STORMS, P. VALCKE & E. KINDT, "Rage against the machine: Does machine-to-machine communication fall within the scope of the confidentiality principle?", *International Journal of Law and Information Technology Law*, 2019, p. 372.

ni une messagerie électronique classique. C'est son choix. Mais ce choix est régi par la loi applicable à la correspondance. En droit international privé, cette dernière relève *a priori* de la protection de la vie privée, et par conséquent du statut personnel[38]. En conséquence, s'applique donc en principe dans les pays d'Europe continentale la loi de la nationalité de la personne[39] ; tandis que, dans les systèmes de droit international privé des pays de *Common Law*, elle relève de la loi du domicile de la personne[40]. C'est la loi applicable au statut personnel qui déterminera la légalité du choix de recourir à de tels services particulièrement furtifs. Ceci, toutefois, sans préjudice de l'application immédiate d'éventuelles lois de police. Or, en la matière, il est probable qu'il y en ait[41], et que ce soit donc elles, selon une application territoriale, qui régissent la matière. A titre d'exemple, en France, l'offre de services de communication électronique est réglementée. La fourniture d'un tel service sur le territoire français pourrait par conséquent relever des dispositions du Code des postes et des communications électroniques, qui soumet à une déclaration préalable l'exercice d'une telle activité[42], et qu'il ne serait pas absurde de qualifier de lois de police, pour autant que l'opérateur dispose d'un établissement en France *(Inlandsbeziehung)* ; ce qui, dans la pratique, semble être rarement le cas. En revanche, pour l'utilisateur, le recours à ce type de technologie est libre sur le territoire français, ainsi que le prévoit la loi du 21 juin 2004[43], sous réserve des cas dans lesquels l'État est susceptible de saisir les données pour obtenir une version en clair[44], et des prérogatives de l'autorité judiciaire pour faire de même pour les besoins d'une enquête pénale[45].

Envisageons en revanche le recours à ce type de services en exécution d'un contrat précédemment conclu, spécialement si ce dernier stipule le recours obligatoire entre les parties à un système de communication crypté. Il serait alors logique de considérer que c'est la loi applicable au contrat (*lex contractus*) qui en définira le régime juridique[46]. Le tout, bien évidemment, dans le respect

---

[38] La solution pourrait être différente si la correspondance présente un caractère contractuel, auquel cas son recours entre les parties et la sanction de sa violation devrait logiquement relever, selon nous, de la loi applicable au contrat.

[39] En droit international privé français, le statut personnel relève ainsi classiquement de la loi nationale de la personne depuis le célèbre arrêt *Busqueta* de 1814, sauf disposition contraire désignant la loi de la résidence habituelle de la personne : A. DEVERS, *J-Cl Droit international*, V° *État des personnes : statut individuel*, n° 20 s.

[40] Voir ainsi en droit international privé anglais: J. HILL, M. NI SHUILLEABHAIN, *Clarkson & Hill's conflict of laws*, Oxford University Press, 5th ed., 2016, p. 317.

[41] Il n'existe pas à notre connaissance, pour l'heure, de jurisprudence sur cette question, en France en tous cas.

[42] Article L 33-1 du Code des postes et des communications électroniques.

[43] Article 30 de la loi du 21 juin 2004.

[44] Article 38.

[45] Article 230-1 du Code de procédure pénale.

[46] Voir ainsi, en France, sur le recours au VPN pour le télétravail, et la nécessité pour l'employeur qui conteste le temps de travail invoqué par le salarié au soutien de sa demande de paiement de ses heures supplémentaires de fournir des données de connexion contredisant celui-ci : Soc 27 janvier 2016, n°14.13697.

d'éventuelles lois de police du ou des pays d'établissement ou de situation des parties, avant et pendant que lesdites communications n'aient lieu. En droit français le dispositif technique devra par exemple être utilisé dans le respect du régime de déclaration administrative préalable imposé au prestataire de service cryptographique, et d'autorisation en cas de transfert vers un État étranger[47].

De façon différente, si l'avocat et son client communiquent entre eux de façon protégée en usant d'outils de discrétion numérique, il paraît logique de considérer que le régime de cet usage relève, en tant que prérogative du secret professionnel et du respect des droits de la défense, de la loi applicable à la procédure (*lex fori*). Cette dernière devra nécessairement être conforme à l'ordre public international européen, lequel comprend notamment l'ensemble des exigences tirées du droit à un procès équitable, telles qu'elles s'infèrent des articles 6 de la Convention européenne des droits de l'homme et 47 de la Charte des droits fondamentaux de l'Union européenne.

Enfin, *last but not least,* le recours à un code verbal, graphique ou autre, par des personnes utilisant un moyen de communication non crypté d'une situation différente. Dans cette hypothèse, les personnes communiquent dans un langage naturel en clair, tout en usant d'un stratagème, qui seul permet de comprendre le sens véritable du message. L'exemple historique le plus parfait, est celui de l'annonce du débarquement allié en Normandie sur Radio Londres fut ainsi réalisée à la radio, à travers une citation, devenue célèbre, d'un poème de Verlaine : « *Les sanglots longs des violons de l'automne bercent mon cœur d'une langueur monotone* ». Mais cette technique de discrétion est évidemment employée dans un cadre civil de façon extrêmement courante, car elle constitue la forme la plus simple d'occultation du message. Ce type d'échange, découlant d'un choix personnel de confidentialité, relève à notre sens du régime de la liberté d'expression en vigueur sur le territoire duquel l'échange se déroule[48].

Ce schéma d'analyse peut être reproduit et transposé à toutes formes d'invisibilité numérique, totale ou partielle. L'idée-maîtresse en est simple. La surveillance de masse constitue un péril sérieux pour la vie privée et les libertés. Mais l'avancée constante des technologies de discrétion numérique peut parer, au moins à l'échelle individuelle, à certains de ses inconvénients. La confidentialité peut à travers elle être protégée, sans pour autant qu'il soit nécessaire de reconnaître un authentique droit à l'invisibilité en soi. Le recours à ces techniques relève du régime propre aux droits existants et applicable aux cadre et titre auxquels

[47] Voir ainsi le décret n°2007-663 du 2 mai 2007.

[48] En droit international privé, la liberté d'expression n'est principalement envisagée sur le terrain de la loi applicable qu'à travers son usage injurieux ou diffamatoire. Dans le système français, la loi du 29 juillet 1881 sur la presse constitue ainsi, dans ses dispositions relatives à la diffamation, une loi de police : Cass. Civ 1ère 19 octobre 2004, n°02-15680.

elles sont employées. Ce schéma d'analyse, valable aussi bien en droit international privé, pour identifier la loi applicable notamment, qu'au droit interne, pour déterminer les dispositions légales applicables, ne vaut pour autant ni approbation ni réserve à l'endroit de la surveillance, et de son antagoniste, l'invisibilité. Il constitue un simple paradigme pour qualifier juridiquement l'état de discrétion numérique. Le débat reste ouvert, par conséquent, sur la nécessité ou non de protéger davantage la vie privée et les données personnelles des citoyens contre la surveillance de masse, qu'elle soit privée ou publique.