LES DROITS PRIVÉS DANS L'AGE NUMÉRIQUE : LE RÔLE DES TRIBUNAUX ?

Lord Colin Tyre
Judge,
Supreme Courts of Scotland

Introduction

Au cours des 30 dernières années, les technologies de l'information et de la communication se sont développées à un rythme de plus en plus rapide et étonnante. Internet a transformé notre mode de vie et il ne présente aucun signe de ralentissement. Lorsqu'une organisation telle qu'un court service conclut un contrat pour un nouveau système informatique, la seule chose certaine est que, au moment où vous l'obtenez, vous ne voudrez plus ce que vous pensiez que vous vouliez lorsque vous l'avez commandé.

La loi a eu grand peine à s'adapter à ces développements. Les règles et les principes juridiques conçus avant l'ère numérique ne peuvent pas toujours être appliqués aux technologies de l'information et de la communication. Des nouvelles règles spéciales peuvent être rapidement remplacées par d'autres avancées technologiques. En conséquence, les tribunaux se voient obligés de résoudre les différends qui n'auraient tout simplement pas été survenus il y a peu de temps.

Dans cette session, on se concentre sur le droit privé à l'ère numérique. Dans cet article, je vais considérer certaines des difficultés qui se sont posées concernant l'exercice et la protection des droits privés, et examiner les façons dont ces tribunaux ont traité ce problème. Je vais présenter quelques brefs commentaires sur le rôle continu des tribunaux dans l'élaboration de la loi en réponse aux changements technologiques. Comme l'Écosse est une juridiction relativement petite, bon nombre de ces questions n'ont pas encore été examinées par les tribunaux écossais. Je devrais donc tirer dans une large mesure la jurisprudence anglaise, ainsi que celle de la Cour de justice et de la Cour européenne des droits de l'homme.

Quels droits privés sont affectés?

Je vais commencer par identifier les droits sur lesquels cet article se concentrera.

<u>Droit à la vie privée</u>

Le premier est le droit à la vie privée. Article 8 de la Convention européenne des droits de l'homme exige le respect de la vie privée et familiale. Ce droit est consacré à tous les membres du Conseil de l'Europe. Comme nous le savons, les valeurs incarnées dans l'article 8 s'appliquent également aux litiges entre un individu et l'État, et dans les litiges entre un individu et un autre individu ou un organisme non gouvernemental comme un journal ou une société de médias sociaux.[1] On avait évidemment les droits à la vie privée au Royaume-Uni avant l'adhésion à la Convention des droits de l'homme. Mais en ce qui concerne les cas qui n'impliquent pas une ingérence de l'État, les tribunaux en Angleterre et au Pays de Galles ont jugé nécessaire d'identifier le droit de common law qui est encapsulé dans article 8; comme ces tribunaux ont décidé qu'un délit en common law concernant la violation de la vie privée n'existe pas.[2] La solution, c'était de développer la loi sur l'abus de confiance pour créer un droit d'intenter une action pour abus de l'information privée. Il est important de noter que, dans le premier considérant du nouveau Règlement général sur la protection des données,[3] la protection des personnes physiques à l'égard du traitement des données à caractère personnel est considérée comme un 'droit fondamental'.
Le droit général au respect de la vie privée et le droit plus spécifique à la protection des données à caractère personnel sont également sauvegardés par articles 7 et 8 de la Charte des droits fondamentaux de l'UE.

L'abus de confiance

L'abus de confiance reste un droit d'action distinct. Les informations peuvent être confidentielles sans être privées, et vice versa.

Liberté d'expression

Le droit à la liberté d'expression, protégé par article 10 de la Convention, constitue un autre droit privé important. Ce droit est souvent en conflit avec le droit à la vie privée d'un autre personne dans article 8. Article 10 reconnaît lui-même que le droit à la liberté d'expression doit être exercé de manière responsable et sous réserve des restrictions nécessaires dans une société démocratique pour, entre autres, protéger la réputation ou les droits d'autrui. Mais, encore une fois, le droit de ne pas être diffamé par un autre ne repose pas uniquement sur les droits de la Convention, mais fait partie de droit national dans les juridictions du Royaume-Uni depuis des centaines d'années.

Défis aux droits privés à l'ère numérique

[1] *Campbell c MGN Ltd* [2004] 2 AC 457, Lord Nicholls of Birkenhead, paragraphe 17.
[2] *Wainwright c Home Office* [2004] 2 AC 406.
[3] Regulation (EU) 2016/679

La vie privée

Certains aspects des technologies de l'information et de la communication présentent des risques particuliers d'interférence avec les droits privés. Le plus évident est l'avènement de 'big data': la capacité des ordinateurs d'effectuer des recherches, de traiter d'énormes quantités de données et de proposer des modèles dont l'identification serait au-delà de la compétence humaine. Une autre est le problème de la 'persistance': une fois que l'information est publiée, elle accessible pour toujours. Sans contrôle, ces aspects des technologies de l'information et de la communication peuvent être exploités par les processeurs de données publics et privés.

Interférence de l'État

Peut-être le plus controversé est le conflit entre les droits de la vie privée et l'exercice par l'état de la collecte d'informations par voie électronique. Au Royaume-Uni, ce conflit est loin d'être résolu. On peut au moins dire que l'exercice des pouvoirs de collecte d'informations de l'État est devenu plus transparent qu'auparavant. Cela s'explique peut-être en partie par les activités des dénonciateurs ; c'est tout récemment que le Royaume-Uni a expressément admis l'existence de Government Communications Headquarters (GCHQ), son centre de collecte et de traitement de l'information, mais il s'explique aussi par le travail du Investigatory Powers Tribunal (Tribunal d'enquête) qui enquête et décide des affaires impliquant des plaintes que les autorités publiques ou organismes chargés de faire respecter la loi ont agi de manière illégale et ont ainsi enfreint les droits à la vie privée ou d'autres droits de l'homme. Ce tribunal peut considérer des questions de sécurité délicates en audience publique, par exemple en les traitant en supposant que les allégations du plaignant sont vraies, sans demander à organismes chargés de faire respecter la loi de confirmer ou de nier les allégations. Le tribunal peut statuer en principe avant l'examen nécessaire des faits en privée. Ce pratique a entraîné une plus grande précision de la divulgation par le gouvernement britannique sur ses pratiques concernant la collecte de renseignements, sous la forme de codes de pratique. Les organismes chargés de faire respecter la loi se sont engagées à respecter ces codes de pratique.

Mais le problème n'est pas résolu si les pratiques ouvertement divulguées sont contraires au droit européen. La conservation des données 'en vrac' est particulièrement controversée, parce que ces données peuvent être collectées de façon ouverte ou secrète. Les données 'en vrac' comprennent à la fois des données personnelles en vrac, c'est-à-dire des informations biographiques, y compris des activités commerciales et financières, des communications et des voyages, ainsi que des données de communications en vrac, qui peuvent inclure l'emplacement des téléphones fixes, et information sur l'emplacement des appels effectués ou reçus (mais pas le contenu des communications), ou l'emplacement

d'un ordinateur utilisé pour accéder à Internet (mais pas l'historique de navigation précis).

Dans le cas de *Digital Rights Ireland*,[4] la Cour de justice a déclaré une directive de 2006 [5] invalide. Cette directive exige que les fournisseurs de services de communication électronique conservent des données en vrac pendant une période de six mois à deux ans pour les États membres dans la recherche, la détection et la poursuite d'infractions pénales graves. Le gouvernement du Royaume-Uni a répondu à cette décision par adopter à la hâte une législation d'urgence, Data Retention and Investigatory Powers Act 2014 (' DRIPA'). Cette loi a rétabli le droit des autorités publiques d'exiger des fournisseurs de services de communication électronique de conserver les données pendant 12 mois, pour de nombreux emplois au-delà de l'enquête et la poursuite des infractions pénales graves. Cependant, la loi de 2014 avait une date d'expiration, la fin de 2016.

La validité de DRIPA a été contestée comme contraire parce qu'elle irait à l'encontre des articles 7 et 8 de la Charte des droits fondamentaux.[6] David Davis, un député conservateur, et Tom Watson, un député travailliste, entre autres, ont intenté l'action; M Davis a ensuite dû se retirer en tant que demandeur quand il était nommé ministre responsable pour le Brexit. Les demandeurs étaient particulièrement préoccupés par les dispositions de DRIPA qui permettaient le recouvrement des données relatives aux communications privilégiées entre avocat et client. Le tribunal de première instance a jugé favorablement la contestation et a rejeté DRIPA dans la mesure où elle n'a pas respecté le droit de l'UE. En appel, la Cour d'appel a posé une question préjudicielle à la Cour de justice. L'affaire a été entendue avec une question préjudicielle de la Suède, et la décision de la Cour a été rendue le 21 décembre 2016.[7]

La Cour a confirmé l'approche qu'il avait adoptée dans *Digital Rights Ireland*, affirmant que le droit communautaire empêchait la législation nationale de prescrire la conservation générale et indiscriminée des données. La protection du droit fondamental de respect de la vie privée exigeait que les dérogations ne s'appliquaient que dans la mesure strictement nécessaire. Étant donné que les données, dans son ensemble, pourraient permettre des conclusions précises sur la vie privée des personnes concernées, l'ingérence de l'Etat devait être considérée comme particulièrement grave. La lutte contre la criminalité grave est le seul objectif capable de la justifier. La Cour a ajouté que, sauf dans les cas d'urgence, il était essentiel que l'accès aux données soit soumis à un examen préalable effectué

[4] Digital Rights Ireland Ltd c Minister for Communications, Marine and Natural Resources, Ireland (Case C 293/12) [2015] QB 127

[5] Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications

[6] Davis & Others c Secretary of State for the Home Department [2016] 1 CMLR 48; [2015] EWCA Civ 1185

[7] Affaires jointes C-203/15 *Tele2 Sverige AB c Post-och Telestyrelsen* et C-698/15 *Secretary of State for the Home Department c Watson & Others*

par un tribunal ou un organisme indépendant. De toute évidence, les opinions de la Cour n'étaient pas indûment influencées par les atrocités terroristes qui se sont produites dans différents États membres puisqu'il a rendu sa décision dans *Digital Rights Ireland*.

L'affaire est maintenant renvoyée devant la Cour d'appel. Bien que DRIPA ait expiré à la fin de 2016, la décision de la Cour de justice est d'une importance majeure, car le 29 novembre 2016, une nouvelle loi, Investigatory Powers Act 2016, a reçu la sanction royale. Cette loi, joyeusement surnommée Snooper's Charter (ou 'la Charte des fouineurs') par les médias, vise à fournir un régime ultramoderne pour l'exercice des pouvoirs d'enquête par les autorités publiques au Royaume-Uni. Les opposants affirment que les vastes pouvoirs dans la loi de 2016 ont les mêmes défauts que son prédécesseur et, par conséquent, qu'il est également incompatible avec les décisions de la Cour de justice. La nouvelle loi n'est pas encore entrée en vigueur. Le gouvernement du Royaume-Uni est en consultation sur les termes de divers projets de codes de pratique pour accompagner la législation, mais on remarque l'absence d'un code de pratique concernant la conservation de données en vrac. Cette question est mise en suspens en attendant l'arrêt de la Cour d'appel.

Le départ du Royaume-Uni de l'Union européenne n'est pas non plus susceptible de changer la position actuelle. Bien que les arrêts de la Cour de justice n'aient plus d'effet contraignant sur le Royaume-Uni, et le Parlement du Royaume-Uni sera libre d'adopter une législation différente des jugements rendus avant la date d'entrée en vigueur de Brexit, cela ne signifie pas que le Royaume-Uni aura la liberté de suivre son chemin. Il faudra encore partager des données avec les États membres de l'UE et ne pourra le faire que s'il peut fournir 'un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'Union'.[8]

Une autre question litigieuse qui intervient plus directement avec les droits privés est ce qui est mentionné dans le jargon de sécurité en tant que l'exploitation de réseau informatique, ou, comme tout le monde l'appelle, un piratage. La mesure dans laquelle les agences de renseignement du Royaume-Uni piratent les ordinateurs a fait l'objet d'une demande auprès du Investigatory Powers Tribunal par un certain nombre de fournisseurs de services Internet dans *Privacy International* et *Greennet Ltd*.[9] L'une des conséquences de l'introduction de l'affaire était que les organismes de renseignement ont reconnu publiquement pour la première fois que certaines activités de piratage étaient continuées, mais certaines activités, telles que la suppression des vulnérabilités dans un ordinateur cible, n'étaient toujours 'ni confirmées ni refusées'. Dans cette affaire, l'une des

[8] *Schrems c Data Protection Commissioner* (Case C-362/14), paragraphe 96.
[9] *Privacy International c Secretary of State for Foreign and Commonwealth Affairs; Greennet and Others c Secretary of State for Foreign and Commonwealth Affairs* [2016] UKIP Trib 14_85-CH

principales questions était de savoir si les mandats autorisant le piratage de catégories de cibles non identifiées par leur nom avaient contrevenu à des protections légales de longue date contre les mandats généraux. Le Tribunal a estimé que ce n'était pas le cas, et la tentative des requérants de faire une demande de contrôle judiciaire n'a pas réussie, la Haute Cour ayant jugé que les décisions du Tribunal ne font pas l'objet d'un contrôle judiciaire.[10] La nouvelle loi, Investigatory Powers Act 2016, prévoit expressément que des mandats sont accordés pour des 'interférences ciblées en matière d'équipement'. Le Tribunal pourrait devoir reconsidérer cette question.

Interférence non étatique

Je me concentre jusqu'à présent sur l'ingérence par l'État dans le droit à la vie privée des individus. Des occasions d'interférence par des individus et par des entités non étatiques sont créés par l'ère numérique. L'affaire de la Cour d'appel anglaise, *Vidal Hall c Google Inc*,[11] est un exemple intéressant. On avait trois utilisateurs d'ordinateurs Apple comme demandeurs dans ce cas. Quand ces demandeurs utilisaient le navigateur Safari et découvraient que les publicités leur étaient évidemment ciblées apparaissaient sur leurs écrans d'ordinateur. Les demandeurs prétendaient que cela ne pouvait que signifier que Google recueillait des informations privées sur leur historique de navigation, contrairement à sa position publiquement déclarée que cela ne serait pas fait à moins qu'un utilisateur de Safari n'en consentie expressément.

L'affaire a été portée devant le tribunal en tant que demande des demandeurs pour autorisation en vertu des règles de procédure civile anglaise pour signifier le bref sur Google en Californie. La question légale à régler, c'était de savoir si l'abus d'informations privées était correctement classé comme un acte délictuel en droit anglais (et c'est le cas). Mais certaines autres questions découlant de la décision du tribunal. Il a été confirmé que la violation de la confiance et l'abus de l'information privée étaient deux motifs d'action distincts avec des fondements juridiques différents. Le tribunal a également noté que la directive sur la protection des données[12] conférait le droit de recouvrer des dommages-intérêts en cas de détresse (en plus des pertes financières) - un droit qui délibérément n'a pas été transposé dans la législation nationale du Royaume-Uni. Dans ces circonstances, il a été décidé que l'article 47 de la Charte des droits fondamentaux (droit à un recours effectif) était engagé et que le tribunal devait empêcher la disposition nationale d'avoir un effet contraire.

[10] *R (Privacy International) c Investigatory Powers Tribunal* [2017] EWHC 114 (Admin)
[11] [2016] QB 1003
[12] Directive 95/46/EC du 24 octobre 1995

Une autre question soulevée était de savoir si les informations générées par le navigateur relevaient de la définition de 'données personnelles'. Google a soutenu que cette information prise elle-même était anonyme: l'individu ne pouvait pas être identifié et Google l'a séparé des autres données telles que les détails du compte de messagerie. Le tribunal ne devait pas trancher cette question, mais a estimé qu'il était suffisamment plausible, et permettait la poursuite de l'affaire. Le tribunal a donné son autorisation pour les demandeurs de signifier le bref en Californie.

Dans le cas de *Mosley c Google Inc*,[13] une forme de violation quelque peu différente de la législation sur la protection des données était au cœur du litige en l'espèce. Les antécédents de l'affaire seront familiers: Max Mosley, l'ancien président de la Fédération Internationale de l'Automobile, a poursuivi avec succès l'éditeur de la News of the World pour avoir violé sa vie privée en imprimant des photographies de lui engager dans une activité sexuelle. Certaines images restaient disponibles sur Internet et pouvaient être consultées à l'aide des moteurs de recherche. Ils sont devenus des 'vignettes', c'est-à-dire des images de taille de fichier réduites, produites par une recherche Google. Lorsque M Mosley l'a découvert, et ses avocats ont signifié des avis en vertu de la loi sur Google, en l'obligeant à cesser de traiter les images. Google a refusé pour diverses raisons, y compris qu'il n'était pas le contrôleur des données. M Mosley a poursuivi une nouvelle fois; cette fois, il a demandé des dommages-intérêts en vertu de la loi britannique sur la protection des données en cas de détresse causée par le traitement par Google de ses données personnelles. À l'heure actuelle, il avait été établi par le jugement de la Grande Chambre dans l'affaire *Google Spain*[14] qu'un fournisseur de services Internet tel que Google était effectivement un contrôleur des données, de sorte que la défense n'était pas disponible.

Au lieu de cela, Google a plaidé sans succès qu'il est tombé dans une exemption pour casser des informations en tant qu'intermédiaire (comme il le fera, par exemple, en ce qui concerne un courrier électronique envoyé par une personne à l'autre), ou, alternativement, ce que M Mosley cherchait dans cette affaire équivalait à une obligation générale de surveillance de la part de Google, que les États membres n'avaient pas le droit d'exiger. Encore une fois, le juge ne devait pas déterminer ces questions, mais il a simplement décidé si l'affaire avait une vraie perspective de succès. Il a décidé qu'il l'avait fait, et que les questions étaient d'intérêt public général, et l'affaire a eu lieu.

La diffamation et la liberté d'expression à l'ère numérique

[13] [2015] 2 CMLR 689
[14] *Google Spain SL c Agencia Española de Protección de Datos* (Case C-131/12)

Le conflit entre la liberté d'expression et le droit à la protection de la réputation n'est pas nouveau. Il est pleinement reconnu dans la Convention des droits de l'homme. Au Royaume-Uni, la loi de 1998 sur les droits de l'homme (Human Rights Act 1998) comprend une disposition[15] qui garantit que, en règle générale, un tribunal ne peut, en règle générale, accorder une ordonnance (comme une injonction ou, en Écosse, une interdiction) restreignant le droit dans la Convention à la liberté d'expression sans avoir donné la personne contre laquelle l'ordonnance doit avoir l'occasion d'être entendue.

L'ère numérique a créé de nouveaux défis pour les lois sur la diffamation. On peut accéder aux publications mondiales avec un ordinateur ou un smartphone, ce qui, avec l'effet désinhibant de l'anonymat comparatif, a permis de créer et de partager du contenu diffamatoire qui précédemment, en raison du contrôle éditorial, n'auraient jamais vu le jour. L'auteur est bien sûr responsable de diffamation de la manière habituelle, s'il peut être identifié et s'il mérite d'être poursuivi. Mais nos juridictions au Royaume-Uni ont dû aborder la question de la responsabilité des intermédiaires: les hébergeurs web; les facilitateurs des forums de discussion en ligne et les commentaires sur les articles; et, le plus controversé de tous, les moteurs de recherche. L'équilibre entre la protection légitime de la réputation et la suppression de la liberté d'expression s'est avéré difficile à frapper. Au Royaume-Uni, la réponse actuelle est un mélange de solutions locales et des solutions inspirées de l'UE.[16] En vertu de l'article 1 de la Loi de diffamation de 1996 (Defamation Act 1996, qui ne concerne pas uniquement la communication numérique), une personne a une défense s'il montre qu'il n'était pas l'auteur, le rédacteur en chef ou l'éditeur de la déclaration dénoncée; qu'il a pris soin de sa publication; et qu'il ne savait pas et n'avait aucune raison de croire que ce qu'il a causé ou contribué à la publication d'une déclaration diffamatoire. Un certain nombre de fournisseurs de services Internet ont argumenté avec succès qu'ils n'étaient pas l'auteur, l'éditeur ou l'éditeur du matériel dénoncé. Dans *Metropolitan International Schools Ltd c Designtechnica Corp*,[17] Eady J a estimé que les extraits apparaissant dans une recherche Google ne constituaient pas une 'publication' en raison de la difficulté réalisable de contrôler ce qui apparaissait en réponse aux termes de recherche d'un utilisateur. Dans *McGrath c Dawkins & Others*,[18] la cour a jugé que Amazon n'était pas l'éditeur de commentaires prétendument diffamatoires dans les revues de livres, mais le juge a permis de se demander si des soins raisonnables avaient été pris pour être jugés.

Une protection distincte pour les 'services de la société de l'information' est assurée par le règlement de 2002 sur le commerce électronique (directive CE). La défense disponible dépend du degré d'implication de l'intermédiaire. 'Mere

[15] Section 12
[16] For a recent discussion, see the Scottish Law Commission Discussion Paper No 161 on Defamation (2016)
[17] [2011] 1 WLR 1743
[18] [2012] EWCA 83

conduits', ou simple transport, comme les services qui transmettent mais ne stockent pas les emails, attirent l'immunité complète. Les fournisseurs de services de forme de stockage dite 'caching', où les informations sont stockées pour une transmission efficace, obtiennent l'immunité si certaines diverses conditions sont remplies. Les fournisseurs de services d'hébergement Web sont protégés contre la responsabilité civile et pénale s'ils démontrent qu'ils ne connaissaient pas exactement les informations 'illégales', qu'ils ne connaissaient pas les faits ou les circonstances dont il aurait été évident que l'information était illégale, et en prenant conscience, ils ont agi rapidement pour supprimer ou désactiver l'accès à cette information. La Cour de justice a jugé, dans le cadre de la violation de la marque de commerce, que cette défense est disponible pour un moteur de recherche, à condition que son rôle soit 'purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des données qu'il stocke'.[19]

L'article 5 de la loi de diffamation de 2013 (Defamation Act 2013) prévoit une autre protection spécifique pour les opérateurs de sites Internet, en Angleterre et au Pays de Galles (mais pas en Écosse). Un opérateur défend une action pour diffamation s'il montre qu'il n'a pas posté la déclaration dénoncée. Cette défense est toutefois vaincue si le demandeur montre qu'il n'a pas été possible d'identifier le participant; le prestataire a donné à l'opérateur un avis de plainte; et l'opérateur n'a pas répondu rapidement à la plainte. Ces dispositions de base sont énoncées dans des règlements,[20] qui spécifient entre autres, comment se plaindre, comment l'opérateur doit répondre initialement, ce que l'opérateur doit faire si le participant originale de l'affiche ne réagit pas, et ainsi de suite. Le but est de trouver l'équilibre désiré entre la protection de la personne qui se plaint, et la liberté d'expression, mais la procédure est si prescriptive que l'on soupçonne que de nombreux opérateurs adopteront le moyen le plus simple de retirer le matériel litigieux au détriment potentiel de la liberté d'expression.

Incertitudes persistantes

Il y a inévitablement des anomalies et des incertitudes avec tant de tentatives différentes pour aborder la question du contenu diffamatoire en ligne. Il n'est pas clair, par exemple, si la responsabilité est attachée à un lien hypertexte vers un site web contenant du contenu diffamatoire; au Canada, il a été jugé que cela ne le ferait que si le texte indique l'adoption ou l'approbation du texte hyperlié.[21] Sur d'autres questions, les différentes juridictions ont pris des diverses décisions. En Nouvelle-Zélande, la Haute Cour a refusé de radier une affirmation que Google était éditeur d'extraits et d'hyperliens pour des informations sur le contenu diffamatoire.[22] Dans une affaire avec des faits quelque peu bizarres, la Cour

[19] *Google France c Louis Vuitton Malletier* [2010] ECR I-2417.
[20] Defamation (Operators of Websites) Regulations 2013
[21] *Crookes c Wikimedia Foundation Inc* [2011] SCC 47
[22] *A c Google New Zealand Ltd* [2012] NZHC 3252

suprême de l'Australie du Sud a estimé que Google était un éditeur d'extraits et de résultats de recherche auto-compliqués diffamatoires dans des circonstances où ils n'avaient pas été abaissés dans un délai raisonnable après la présentation d'une plainte.[23]

Et il se peut qu'il ne soit même pas suffisant de déposer une déclaration diffamatoire rapidement après la plainte. Dans *Delfi c Estonie*,[24] un grand portail d'information sur Internet a publié un article critique sur une compagnie de traversier et un membre de son conseil d'administration. Cela attirait des commentaires dont beaucoup comportaient des menaces personnelles et des déclarations humiliantes et diffamatoires dirigées contre le membre du conseil d'administration. La Grande Chambre de la Cour européenne des droits de l'homme a confirmé le jugement de la Cour suprême de l'Estonie selon lequel le portail Internet était l'éditeur des commentaires qui, en raison de leur contenu, n'attiraient pas la protection de l'article 10. Le portail d'information a été géré professionnellement, sur une base commerciale, et a cherché à attirer des commentaires sur les articles publiés. De plus, le portail exerçait un degré important de contrôle sur les commentaires publiés et son rôle était supérieur à celui d'un fournisseur de services passif. L'obligation de supprimer ces commentaires sans délai suite à la publication (même avant la réception d'une plainte) ne constituait pas une ingérence disproportionnée sur la liberté d'expression de Delfi.

Autres droits privés

La protection de la réputation contre la diffamation n'est pas la seule situation dans laquelle le droit à la liberté d'expression dans article 10 peut entrer en conflit avec les intérêts des autres. Certains exemples incluent les discours haineux, le 'revenge porn', et d'autres abus de médias sociaux qui ne constituent pas une diffamation. Une solution, qui a été adoptée dans une certaine mesure en Écosse, consiste à criminaliser certains types d'activités de ce genre. Mais c'est une stratégie risquée. La pression populaire tend à influencer ces types de loi, et ces lois peuvent entraîner une violation des droits de l'article 10 si elles ne sont pas soigneusement examinées.

Je note que la nouvelle loi sur l'économie numérique (Digital Economy Act 2017, qui s'applique à l'Écosse) comprend, à la suite d'un amendement tardif à la Chambre des Lords, une obligation pour le gouvernement d'émettre un code de pratique aux fournisseurs de plateformes de médias sociaux tels que Facebook, contenant des conseils sur les mesures à prendre contre l'utilisation de leurs plates-formes par des individus pour l'intimidation en ligne, et l'insultes ou

[23] *Duffy c Google Inc* [2015] SASC 170
[24] (2016) 62 EHRR 6

l'humiliation d'autrui. Aucune sanction n'est spécifiée. Il reste à voir si cela constitue un moyen efficace de réduire l'abus en ligne de la liberté d'expression et la protection conséquente des droits de l'article 8.

Le rôle des tribunaux

L'image générale qui se dégage de cette vue d'ensemble brève est complexe, c'est une image dans laquelle la législature et le pouvoir judiciaire ont participé à la réponse de la loi aux changements technologiques et numériques. Dans certains domaines, notamment l'interception des communications privées à des fins de sécurité nationale - ou à des fins plus larges - les gouvernements préfèrent considérer l'élaboration de la loi comme une question pour eux et non pour les tribunaux. Mais les gouvernements ne décident pas tous. Les tribunaux sont tenus d'appliquer un droit supranational tel que les décisions des deux cours européennes et les conventions et traités pertinents, et au moins au Royaume-Uni, il est clair que ces défis ont souvent réussi. Si rien d'autre, ils ont obligé le gouvernement du Royaume-Uni de divulguer la mesure dans laquelle il souhaiterait interférer - et entraver - les droits à la vie privée à des fins dépassant ce que beaucoup de gens considéreraient comme une protection essentielle, comme la prévention du terrorisme. Ils ont exposé, par exemple, la mesure dans laquelle le gouvernement souhaiterait, s'il le pourrait, d'outrepasser les garanties telles que la protection accordée aux communications entre un avocat et son client et la confidentialité des sources journalistiques. Mais la participation des tribunaux s'est étendue au-delà faire la lumière sur ces pratiques; en particulier la Cour de justice a adopté une ligne dure sur l'acquisition et la conservation de données en vrac et sans aucun doute, elle a eu une influence sur l'élaboration de la législation nationale sur ce sujet controversé. Lorsque le gouvernement du Royaume-Uni renvoie son attention à la mise en vigueur de la loi sur les pouvoirs d'enquête 2016 (Investigatory Powers Act 2016), elle devra tenir compte des conséquences pour cette nouvelle législation du jugement de la Cour dans l'affaire Watson et en particulier, pour la production d'un code de conduite concernant la conservation des données en vrac. Il sera surprenant que la question ne se retrouve pas devant les tribunaux, qui devra de nouveau examiner la relation entre la législation nationale et les droits fondamentaux protégés par la Convention et la Charte. Concernant des questions en dehors de la sécurité nationale, les tribunaux jouent un rôle tout aussi importants. Une fois de plus, les droits fondamentaux de common law, ainsi que les droits de la Convention et de la Charte, seront invoqués et le cas échéant, devront être protégés. Même lorsque la législature a tenté de fournir des solutions par micro-gestion, comme c'est le cas avec la responsabilité des opérateurs de sites Internet, cela ne peut jamais être une solution complète. Les moteurs de recherche exercent une fonction sociale précieuse - en effet, on peut dire que, à l'ère d'Internet, ils sont une utilité indispensable, mais l'expérience a montré qu'ils peuvent être manipulés pour

produire des interférences néfastes avec les droits à la vie privée. Le développement de la technologie évaluera constamment l'interprétation correcte d'expressions telles que l'éditeur et la publication. De même que les tribunaux ont dû appliquer des concepts créés il y a plusieurs années pour la presse écrite à la diffusion numérique de l'information, des commentaires, des abus, des désinformations délibérées et tout le reste, ils continueront d'appliquer les concepts créés pour la technologie du jour à la technologie de deux, cinq ou dix ans dans le futur, qui sera tout aussi difficile.

De nouveaux dangers?

J'offre une autre question controversé pour considération. Le sujet de 'fake news' a été mis en évidence au cours de la dernière année, notamment en raison de l'influence présumée d'informations inexactes diffusées en ligne lors de l'élection présidentielle américaine de 2016. Les expressions 'fake news', et 'alternative facts' (faits alternatifs) ont donné lieu à des commentaires légers dans les médias traditionnels, mais ils sont vraiment très sérieux. Lorsqu'une partie substantielle de la population reçoit des informations au moyen de Twitter, dans lequel les problèmes complexes sont réduits à quelques mots qui rendent la fausse représentation des faits pratiquement inévitable, on est concerné que le processus démocratique peut être submergé par la propagande extrémiste, comme cela s'est produit dans un passé pas trop lointain.

Ma question est simplement la suivante: est-ce qu'un droit de droit privé des personnes engagées par la promulgation et la répétition d'affirmations factuelles non-diffamatoires mais fausses? Si c'est le cas, quel serait le fondement d'un tel droit? L'article 8 de la Convention est-il suffisamment large pour englober une ingérence dans la vie personnelle consistant à dire des mensonges au monde en général? Probablement pas : d'habitude, il serait difficile d'établir le statut de 'victime'. Existe-t-il donc un besoin d'une nouvelle forme d'actio popularis, reconnaissant un intérêt public conféré à un individu pour contester la publication de la désinformation et l'empêcher d'exercer une influence maligne? Au Royaume-Uni, la Cour suprême a démontré sa volonté de s'écarter de l'ancienne notion de titre à poursuivre (title to sue) en faveur d'une notion plus souple d'intérêt suffisant (sufficient interest).[25] Est-ce que cela représenterait une ingérence totalement injustifiable dans la liberté d'expression, ne relevant pas de l'une des catégories énumérées dans article 10 où cette liberté peut légitimement être restreinte?

L'expérience récente montre que les tribunaux sont parfois appelés à s'attaquer aux problèmes que les politiciens hésitent à aborder, conscients de la réaction possible de la presse (y compris la réaction des fournisseurs de fake news). Il ne

[25] Voir, par exemple, *AXA General Insurance Ltd c HM Advocate & Others* [2012] 1 AC 868

semble pas y avoir suffisamment d'appétit de la part des fournisseurs de médias sociaux tels que Facebook et Twitter pour faire quoi que ce soit à moins et jusqu'à ce qu'ils soient légalement obligés de le faire. Le problème semble se développer. Un jour, quelqu'un demandera à un juge de prendre des mesures pour empêcher la répétition d'un élément de 'fake news' non diffamatoires. Quelle sera la réponse?