Défendre les vivants ou les morts ? Controverses sous-jacentes au droit des données *post-mortem* à travers une perspective comparée franco-américaine

Lucien Castex
Edina Harbinja
Julien Rossi

Résumé

Etre sur Internet, c'est exister comme un être de données constituant des profils qui doublent l'existence des individus physiques et leur survivent. A l'avenir, Internet est donc appelé à contenir plus de données *post-mortem* que de données personnelles relatives à des personnes vivantes. Quel sort réserver à ces données ? Pendant longtemps, le droit était resté muet sur cette question, le droit des données personnelles s'arrêtant à la mort de la personne. L'analyse comparée de l'évolution du droit aux Etats-Unis et en France permet de déceler une différence de conception entre une approche basée sur le référentiel du droit à la vie privée et à la protection des données, et celle qui s'inspire du régime successoral et patrimonialise les données *post-mortem*.[1]

Mots-clefs : traces numériques, droit de la protection des données, droit de la succession, mort numérique

[1] Cet article a pour cadre le Programme Eternités numériques: Les identités numériques post mortem et les usages mémoriaux du web (ENEID), soutenu par l'Agence Nationale de la recherche (Sociétés innovantes 2013), 2014-2018. Voir notamment http://eneid.univ-paris3.fr/ et http://www.costech.utc.fr/spip.php?article120 .

Le numérique transforme les modes de production et de diffusion de l'information, et influence jusqu'au fonctionnement de la démocratie (Cardon, 2010). Il génère également des masses croissantes de données qui mettent à l'épreuve les modes de régulation traditionnels (Huet et Dreyer, 2011). L'évolution des pratiques, la quantification de soi (Lanzing, 2016) et l'internet des objets (G29, 2014) ne font que renforcer ce phénomène.

Etre sur Internet, c'est exister comme un être de données : nom réel ou pseudonymique, discours, correspondance, sur différents supports. Etre sur Internet, c'est être de son vivant mais aussi perdurer dans la mort, le numérique n'épousant pas la temporalité du corps physique de l'être humain. A terme, le nombre de profils constitués de traces numériques, en ligne ou bien dans les bases de données informatisées inaccessibles au public (fichiers RH d'entreprises, profils marketing établis par des *data brokers*, archives d'établissements scolaires, etc.) est appelé à dépasser le nombre de profils relatifs à des personnes vivantes. Ainsi perdurent des données que l'on croyait depuis longtemps oubliées : comptes inactifs, anciens écrits, commentaires. Ces informations peuvent remonter au détour d'un lien ou du référencement d'un moteur de recherche.

En parallèle, nous pouvons observer le développement de nouvelles pratiques funéraires faisant usage d'outils numériques. Des pages Facebook se créent à la mémoire des défunts, des messages sont envoyés à partir de leurs anciens comptes des défunts, des cimetières virtuels parfois gérés par des entreprises spécialisées (Georges et Julliard, 2014 et 2016), comme Paradis Blanc (Bourdeloie, 2015) sont constitués. Ces nouvelles pratiques font naître de nouveaux problèmes juridiques faisant l'objet d'une réglementation récente, qui est l'objet de l'analyse du présent article.

Les médias états-uniens et européens ont largement diffusé l'information sur une des premières affaires impliquant des données *post-mortem*. Il s'agissait de l'affaire *In Re Ellsworth*, dans laquelle l'entreprise Yahoo !, fournisseure de services de messagerie électronique, avait refusé de donner à la famille de Justin Ellsworth, fantassin de marine américain mort au combat en Irak, accès à son compte de messagerie électronique. Selon Yahoo !, les conditions générales d'utilisation du service, conçues selon cette entreprise pour garantir

la vie privée, n'auraient pas permis que de tierces personnes accèdent au compte d'un utilisateur après sa mort. Toujours selon cette entreprise, une loi des Etats-Unis sur la vie privée dans les communications électroniques[2] leur interdisait de divulguer les communications personnelles d'un utilisateur sans un ordre d'un juge. La famille du soldat rétorquait qu'en tant qu'héritiers, ils devraient se voir accorder l'accès à l'intégralité de son compte, incluant les courriels reçus et expédiés, qui contenaient potentiellement ses dernières paroles. Yahoo ! ayant une politique de non-succession, il y avait par ailleurs un danger que le compte du soldat Ellsworth soit effacé.

Le juge permit à Yahoo ! d'appliquer ses règles de confidentialité en permettant à l'entreprise de ne pas communiquer l'identifiant et le mot de passe du compte aux héritiers. Cependant, il donna l'ordre à Yahoo ! de permettre l'accès au contenu du compte par la famille du défunt en leur envoyant la copie des e-mails gravés sur un CDROM. Or, comme rapporté par la presse, l'entreprise ne copia dans un premier temps sur le CDROM que les e-mails que le défunt avait reçus, et il fallut que la famille porte de nouveau plainte avant qu'elle n'obtienne également une copie imprimée des e-mails expédiés. Cette affaire illustre ainsi clairement l'essentiel des problèmes autour de la transmission *post-mortem* de courriers électroniques et d'autres biens numériques. Selon l'analyse faite par Lilian Edwards et Edina Harbinja (2013), une des façons de comprendre cette affaire est que Yahoo ! était propriétaire des copies des courriels stockés sur leurs serveurs, mais était lié par l'ordre du juge exigeant que l'entreprise offre un accès aux informations qu'ils contenaient. Cette lecture peut être justifiée par la division traditionnelle du droit états-unien de la correspondance, séparant la propriété par Yahoo ! de l'aspect matériel des e-mails, du droit d'auteur sur leur contenu, transmis aux héritiers à la mort de leur auteur. L'autre interprétation proposée par Lilian Edwards et Edina Harbinja (2013) se fonde sur le fait que les e-mails appartiennent bien à leur auteur de leur vivant, et que leur droit de propriété se transmet aux héritiers à la mort de celui-ci. Elles considèrent cependant qu'il est peu probable que le juge ait retenu cette dernière interprétation, car il aurait alors ordonné l'accès à l'intégralité du compte du défunt en considérant que les droits des héritiers prévalent sur les termes des conditions générales

2 La Electronic Communications Privacy Act de 1986

d'utilisation. Nous pouvons donc en conclure que le juge a bien confirmé la propriété de Yahoo ! sur les e-mails du défunt, tout en consacrant un droit d'accès au contenu de cette correspondance pour les héritiers. Dans le fond, cette affaire n'a donc pas permis de dégager de grands principes ou lignes directrices pouvant être appliquées à d'autres cas.

En 2012, une fille de 15 ans est morte à Berlin dans une collision avec une rame de métro. Ses parents ont alors souhaité savoir s'il s'était agi d'un suicide, et ils ont voulu vérifier si elle n'avait pas subi de harcèlement en ligne en accédant à ses messages Facebook. La mère avait ses identifiants, mais ne put se connecter car une amie de celle-ci avait déjà notifié son décès au réseau social. Facebook avait alors désactivé le compte, et refusé de transmettre à la mère les conversations que sa fille avait eues. Et si, en première instance, un juge avait déclaré que la mère pouvait hériter du contrat que sa fille avait de son vivant avec Facebook, la Cour d'Appel de Berlin[3] décida que quelles que soient les règles en matière de succession pour les contrats, le droit allemand relatif à la vie privée lui interdisait l'accès aux messages de sa fille. Cette affaire a fait titrer le journal allemand *Die Welt* : « La protection des données contre la morale » (Seyffarth, 2017).

Enfin, dans une autre affaire, en Hongrie cette fois, l'Autorité nationale pour la protection des données et la liberté de l'information (NAIH) avait reçu une plainte relative à un cas de harcèlement dans lequel un homme résidant à l'étranger était entré en contact avec une femme hongroise qu'il tenta de convaincre de divorcer pour pouvoir se marier avec lui et qu'il puisse se rendre en Hongrie. Prenant connaissance des échanges, le mari tua sa femme et leurs deux enfants avant de se suicider. Puis, l'homme qui était entré en contact avec la victime via Facebook dévoila à des tabloïds hongrois des extraits de leurs conversations. Il menaça la famille de publier des photos intimes que la victime lui avait envoyées s'ils n'obtempéraient pas à certaines de ses demandes. Suite à cette plainte, la NAIH publia une recommandation (NAIH, 2015) destinée à attirer l'attention des pouvoirs publics sur le flou juridique qui résulte du fait qu'une fois les personnes concernées décédées, le droit des données personnelles qui jusqu'alors protégeait leur vie privée ne s'applique soudainement plus, sans que l'on sache précisément quelles dispositions

3 Landgericht Berlin, 21 U 9/16, 31 mai 2017

légales s'y substituent, notamment pour réglementer leur diffusion.

En effet, en Europe, sauf exception[4] définie en droit national, le droit de la protection des données à caractère personnel – actuellement régi par une directive de 1995[5] puis qui sera régi par le Règlement général de protection des données[6] (RGPD) à partir du 25 mai 2018 –, ne s'applique pas aux données relatives à des personnes décédées[7], laissant aux législateurs nationaux le soin de légiférer en matière de données *post-mortem*.

Quant aux Etats-Unis, ils ont fait le choix, dès les années 1970 (OCDE, 1974), de ne pas bâtir de politique publique et de droit de la protection des données – laquelle a pris en Europe une autonomie aux contours encore flous vis-à-vis du droit à la vie privée (Gonzalez Fuster, 2014) – et de laisser l'essentiel de la régulation des données personnelles à une logique de marché (Rochelandet, 2010). C'est pourtant dans ce pays que, malgré l'absence d'une politique publique nationale de protection des données, les premières lois relatives aux données *post-mortem* ont été adoptées.

Dans quelle mesure les différences de traditions juridiques entre la France et les Etats-Unis ont-elles influé sur les lois régissant les données *post-mortem* qui y ont été adoptées ?

Nous verrons que les Etats-Unis ont d'abord adopté des solutions qui visent à insérer les données *post-mortem* dans une logique successorale en en faisant des actifs numériques accessibles aux héritiers, même si depuis, cet accès a été restreint, notamment sous la pression de l'industrie du Web. En France, qui dispose d'un droit des données personnelles et d'institutions comme la

---

4 Par exemple, le paragraphe 3 de l'article 28 de la loi de protection des données à caractère personnel de Bulgarie (Закон за защита на личните данни) de 2002 modifiée permet aux héritiers de la personne concernée d'exercer son droit d'accès à ses données personnelles

5 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

6 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD)

7 Voir le considérant 27 du RGPD

Commission nationale de l'informatique et des libertés (CNIL) chargés du contrôle de son application, le raisonnement est parti d'une toute autre logique. L'adoption d'une loi de 2016 a inscrit les données *post-mortem* dans le cadre du droit à la protection des données personnelles. Cette loi a écarté l'approche de la patrimonialisation dans une logique successorale pourtant défendue par certains acteurs du débat, tout en en intégrant malgré tout certains éléments. La situation finale, qui se rapproche en pratique et par certains aspects de la solution adoptée aux Etats-Unis soulève comme nous le verrons un certain nombre de questions sur le rôle et la nature du droit à la vie privée comme du droit à la protection des données personnelles, sur lesquelles nous reviendrons en conclusion et qui peuvent être résumées par : de qui le droit des données *post-mortem* défend-il les intérêts ?

AUX ETATS-UNIS : UNE APPROCHE DES DONNEES *POST-MORTEM* SOUS L'ANGLE DES BIENS NUMERIQUES

Le système de protection des données personnelles repose, aux Etats-Unis, sur des bases historiques très différentes de l'approche européenne. Si ses origines remontent à l'époque coloniale et à la jurisprudence autour des quatrième et cinquième amendements, le XIXe siècle vit une étape décisive dans l'invention du droit états-unien de la vie privée (Solove, 2006). En 1890, Samuel Warren et Louis Brandeis publièrent leur article fondateur intitulé « The Right to Privacy » dans lequel ils définirent la vie privée comme étant « le droit général d'un individu à être laissé tranquille »[8]. Ceci fut suivi par le développement de délits d'atteinte à la vie privée, retravaillés par William Prosser (1960) et acceptés en tant que tels dans le *Restatement of Torts*, ouvrage proposant une typologie de référence des délits en *Common Law*. Cette première évolution fut suivie par une série de lois sectorielles (Solove, 2006), les Etats-Unis n'ayant jamais adopté une approche générale et globale de la protection de la vie privée et de la protection des données à caractère personnel tel que celui, fondé sur les libertés fondamentales, qui a vu le jour

8 Traduction des auteurs. Texte original « the more general right to be let alone » (Warren et Brandeis, 1890, p. 205)

en Europe.

Du point de vue de la doctrine, les travaux de recherche montrent que le droit des Etats-Unis ne consacre pas d'un point de vue juridique la notion de vie privée *post-mortem*. Au lieu de cela, le phénomène est encadré par des emprunts épars à divers autres instruments juridiques. La plupart de ces instruments juridiques se concentrent sur les aspects patrimoniaux des données et actifs numériques *post-mortem*. Les aspects non-monétaires, personnels ou liés à la dignité de la personne ne sont traditionnellement pas protégés en tant que tels. (Edwards et Harbinja, 2013b).

Ceci s'explique par le fait que la *Common Law*, tant en Angleterre qu'aux Etats-Unis, a toujours suivi le principe traditionnel *actio personalis moritur cum persona*[9], qui s'applique notamment aux plaintes en diffamation, pour abus de confiance, ou pour licenciement abusif (voir : *Baker v. Bolton (1808)* 170 Eng. Rep. 1033]). Aux Etats-Unis, il s'applique aussi au droit à la vie privée, sauf pour deux exceptions. La première, prévue dans le *Second Restatement of Torts*, est en ce qui concerne les infractions d'appropriation de l'identité d'autrui (*Restatement (Second) of Torts § 6521, 1977*)). La seconde sont les Etats où il existe une protection des droits de publicité, qui incluent le droit à l'image jusqu'à 70 ans après la mort d'une personne (Edwards et Harbinja, 2013b, p. 124). Par ailleurs, il existe aux Etats-Unis une liberté testamentaire garantissant une plus grande autonomie à la volonté du défunt que dans des pays de droit continental comme la France (du Toit 2000, 360; De Waal 2007, 14). La liberté testamentaire aux Etats-Unis reconnaissait donc une forme de vie privée *post-mortem* mais uniquement pour ce qui était des actifs physiques (Harbinja, 2017).

Un certain nombre d'Etats des Etats-Unis ont, suite à la couverture médiatique d'affaires comme l'affaire *Ellsworth* présentée en introduction, été très actifs pour légiférer en matière de transmission des actifs numériques (*digital assets*) à la mort de leur détenteur.

La première phase de ce processus de réglementation a commencé en 2005, et s'est poursuivie sur une période de dix ans durant laquelle une vingtaine

9 Le droit d'ester en matière de droit de la personne meurt avec la personne

d'Etats ont adopté des lois en la matière. Cette phase de réglementation a abouti à l'adoption de lois partielles et fragmentées, ne couvrant que certains types d'actifs comme les courriels ou les comptes de réseaux sociaux numériques, et ne reconnaissant pas de droit à une vie privée *post-mortem*, puisqu'elles permettaient un accès par défaut aux données des défunts, étendant ainsi au monde numérique les logiques traditionnelles du droit des successions (Harbinja, 2017b et Lopez, 2016).

Dans un second temps, un processus d'harmonisation à l'échelle des Etats-Unis s'est enclenché en réponse à cet éparpillement. En juillet 2012, la US Uniform Law Commission (ULC) a chargé un nouveau comité[10] de travailler sur une nouvelle loi capable d'harmoniser le régime applicable aux données (et biens numériques) *post-mortem* en modifiant si besoin les dispositions d'autres lois applicables. Cette nouvelle loi devait autoriser les fiduciaires[11] à accéder aux actifs numériques ainsi qu'à les gérer, les distribuer, les copier ou encore les supprimer. Le projet de Loi sur l'Accès Fiduciaire Uniforme aux Actifs Numériques (*Uniform Fiduciary Access to Digital Assets Acts* – UFADAA) fut publié et diffusé à de multiples occasions (Lopez, 2016).

Les rédacteurs de cette loi eurent à débattre notamment de la définition de la notion de propriété numérique, du type de contrôle que pouvait exercer un fiduciaire, et de la façon de trancher les conflits entre héritiers (ULC, Prefatory Note for the Drafting Committee, 2013).

Dans un premier temps, l'ULC adopta en juillet 2014 un texte permettant un accès par défaut des fiduciaires aux données *post-mortem*, sauf volonté contraire du défunt. Si le testament si ne s'y opposait pas, il pouvait alors donner un accès aux héritiers aux données ayant de la valeur patrimoniale, les autres données faisant le cas échéant l'objet d'une demande de fermeture de compte.

Plusieurs compagnies, comme Google et Facebook, alliées au sein d'un même think-tank appelé NetChoices, ont entrepris à ce moment une intense

10 Le *Committee on Fiduciary Access to Digital Assets*

11 Dans le contexte discuté par le présent article, les fiduciaires sont les personnes désignées par le testament comme devant exécuter les volontés du défunt. Il s'agit d'une forme de mandataire.

campagne de lobbying (Weiner, 2015). Elles proposèrent en 2015 un texte différent : la Loi sur les attentes et les choix en matière de vie privée après la mort (*The Privacy Expectation Afterlife and Choices Act - PEAC*) qui par défaut bloquait l'accès des héritiers aux données du défunt. Sans aller jusqu'à adopter ce dernier, la US Uniform Law Commission adopta la même année certaines des propositions favorables à la vie privée *post-mortem* de l'industrie dans la version révisée de l'UFADAA (*Revised Uniform Fiduciary Access to Digital Assets Acts* : RUFADAA).

Les changements adoptés dans cette version révisée reflètent l'efficacité du lobbying de ces compagnies. Ainsi, le RUFADAA prévoit un accès des fiduciaires restreint au seul catalogue des données du défunt, et non à leur contenu, qui ne peuvent plus faire l'objet d'un accès qu'avec le consentement express du défunt ou bien avec l'injonction d'un juge. Ce mandat ne peut être obtenu que par un procès coûteux.

Les lois proposées par la US Uniform Law Commission, un organisme privé, ne sont pas adoptées par le Congrès des Etats-Unis. Elles sont des propositions, non contraignantes, destinées à aider les Etats fédérés des Etats-Unis à harmoniser leurs lois dans des domaines de compétence n'appartenant pas au gouvernement fédéral. Les Etats peuvent décider d'adopter ces lois ou non.

A l'heure actuelle, la Californie, où sont basées bon nombre de fournisseurs de services en ligne, n'a toujours pas adopté cette loi, ni prévu de l'adopter, selon les informations fournies sur le site de la US Uniform Law Commission. Malgré tout, 37 autres Etats l'ont déjà adoptée[12]. Parmi eux, un certain nombre avaient déjà adopté des lois en matière d'accès aux actifs numériques *post-mortem*.

Au final, le régime américain de transmission des actifs numériques adopté dans la majorité des Etats des Etats-Unis s'inscrit dans une logique successorale et ne reconnaît pas explicitement de droit à la vie privée *post-mortem*. Cependant, ce droit à la vie privée après la mort a été un élément

12 Voir les informations fournies sur le site de la US Uniform Law Commission : http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015) (page consultée le 30 octobre 2017)

central des arguments d'entreprises ayant fait évoluer l'UFADAA vers le RUFADAA. Ce dernier rejoint ainsi partiellement la solution adoptée en France, et ce même si, comme nous le verrons, la réflexion est partie dans ce pays d'une toute autre approche, imbriquée dans des politiques publiques de protection des données personnelles qui n'existent pas aux Etats-Unis.

EN EUROPE : UNE INSERTION IMPARFAITE DANS LE SYSTEME DE POLITIQUE PUBLIQUE RELATIVE A LA PROTECTION DES DONNEES

L'Europe a vu naître les premières lois de protection des données à caractère personnel, dont la toute première adoptée en 1970 en Allemagne dans le Land de Hesse[13]. Il y fut inventé un nouveau terme : la *Datenschutz*, ou « protection des données », qui contrairement à ce qu'il suggère intuitivement ne s'applique pas à toute donnée, mais à celles à caractère personnel. Le terme, popularisé par Spiros Simitis, s'imposa jusqu'à devenir le fondement d'un nouveau droit voisin du droit à la vie privée : le droit à la protection des données personnelles (Hustinx, 2013). Ces efforts répondaient à une inquiétude sur le développement de l'informatique et de bases de données sans cesse plus grandes contenant des informations sur des individus physiques identifiés ou identifiables (Conseil d'État, 1970 ; OCDE, 1974 et Hondius, 1975).

La coalition de cause (Sabatier, 1998), essentiellement constituée de hauts fonctionnaires, qui inventa et défendit à cette époque les principes toujours en vigueur régissant le traitement de données à caractère personnel en Europe, s'est transformée petit à petit en réseaux transgouvernementaux renforcés par la création, dans différents Etats européens, d'autorités administratives indépendantes se voyant octroyer un pouvoir de supervision sur tout ou partie des traitements de données personnelles sur leurs territoires (Newman, 2008). Certains des membres de ce groupe parfois évoqué sous le terme « *privacy community* », comme Jan Pieter Hustinx aux Pays-Bas, Masao Horibe au Japon, Spiros Simitis en Hesse, Louis Joinet et Philippe

13 Hessisches Datenschutzgesetz, 7. Oktober 1970 (GVBl. I S. 625)

Lemoine en France, ou encore Stefano Rodotà en Italie, allaient d'ailleurs rejoindre ou diriger les premières autorités de protection des données à caractère personnel, parmi lesquelles la Commission nationale de l'informatique et des libertés (CNIL), en France, est aujourd'hui l'une des plus influentes.

Les politiques publiques de protection des données se structurent depuis le début des années 1970 autour des ces acteurs qui partagent un référentiel que Charles Raab et Colin Bennett appellent le « paradigme de la vie privée » (Bennett et Raab, 2003, pp. 13-31). Inspiré du libéralisme du philosophe utilitariste John Stuart Mill (Mill, 1989), celui-ci fut par la suite influencé par les thèses de Michel Foucault (1975) et de Gilles Deleuze (1990) sur la surveillance panoptique et la société de contrôle qui font écho à des craintes sur l'influence de la technologie sur la vie privée illustrés par le roman *1984* de George Orwell (Orwell, 1949)[14].

Les autorités de protection des données de l'Union européenne sont aujourd'hui l'armature institutionnelle de cette politique publique. Elles seront chargées, à partir du 25 mai 2018, d'appliquer et de faire appliquer le RGPD, qui succède à la directive de 1995 relative à la protection des données et aux diverses lois nationales.

Que ce soit le RGPD ou les textes l'ayant précédé, ils s'appliquent non pas aux seules catégories de données relatives à la vie privée, à l'intimité, des individus, mais à toute information, quelle que soit sa nature, qui puisse être reliée directement ou indirectement, par exemple par croisement avec d'autres données, à des personnes physiques, ce qui explique que ce droit se soit en partie autonomisé du droit fondamental à la vie privée. Si toute donnée tenant de la vie privée est une donnée personnelle, la réciproque n'est pas vraie.

Mais dès lors que les personnes auxquelles se rapportent ces données décèdent, les autorités de protection des données ne sont, en théorie, plus

14 Pour plus d'informations sur les débats autour de la notion de panoptique et de société de contrôle dans le champ des *Surveillance Studies*, nous vous conseillons la lecture d'un article publié par Bart Simon en 2002 dans *Surveillance & Society* intitulé « The Return of Panopticism: Supervision, Subjection and the New Surveillance » (Simon, 2002)

compétentes pour superviser leur protection. Au Royaume-Uni, pays de *Common Law*, le législateur a même opté pour exclure explicitement les données *post-mortem* du champ de la protection de la vie privée et des données personnelles (House of Lords, 1992 ; Harbinja, 2017), sans d'ailleurs qu'il ne semble pour autant prêt à s'engager sur la voie de l'approche adoptée aux Etats-Unis (Law Commission, 2017). Pour autant, le fait que, comme en Hongrie, des autorités de protection des données aient reçu des plaintes et des demandes relatives à des données *post-mortem* a conduit certaines des ces autorités à produire des guides[15] ou à formuler des recommandations visant à faire évoluer la législation nationale (NAIH, 2015).

En France, la CNIL s'est vue reconnaître des compétences en matière de données *post-mortem* par le nouvel article 40-1 de la loi 78-17 du 6 janvier 1978 modifiée, dite loi Informatique et Libertés. Cette nouvelle disposition, introduite par la loi pour une République numérique[16], fait de la CNIL l'organisme certificateur des tiers de confiance numérique qui pourront enregistrer les directives relatives au sort de leurs données personnelles laissées de leur vivant par les défunts.

Cette insertion, comme nous allons le voir, n'est cependant pas parfaite. Tout d'abord, si nous retrouvons des acteurs comme la CNIL, qui évoque le sujet dans son rapport annuel de 2014, dans l'univers de la réglementation des données *post-mortem*, le droit que ces autorités mettent en œuvre est un droit différent de celui applicable aux données personnelles, qui ne relève ni d'une harmonisation européenne ni du mécanisme de guichet unique mis en place par le RGPD pour éviter que les organismes traitant des données personnelles soient soumis au contrôle de plusieurs autorités nationales de supervision différentes, chacune avec leur interprétation. Ensuite, puisque le sujet touche aussi au droit des successions, nous trouvons également un autre groupe

15 Voir sur le site Internet de la CNIL : https://www.cnil.fr/fr/mort-numerique-peut-demander-leffacement-des-informations-dune-personne-decedee-0 (page consultée le 19 octobre 2017)

16 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

d'acteurs très impliqués : les notaires, qui sont généralement absents du champ de la protection des données personnelles. Enfin, comme nous le verrons, la question de savoir si nous devons considérer le sort des données *post-mortem* sous l'angle de la vie privée fait débat. Faut-il verrouiller l'accès des données des défunts au nom d'une attente raisonnable qu'ils auraient eu de leur vivant à ce que ces données restent inaccessibles au public, à la recherche scientifique et historique, voire à leurs proches ? Faut-il, toujours dans une optique de protection de l'intérêt du défunt, appliquer un régime de droit mémoriel interdisant l'atteinte à la mémoire des morts, comme c'est notamment le cas en Hongrie[17] ? Ou bien faut-il protéger les intérêts des héritiers en facilitant leur accès aux données personnelles des défunts, considérées cette fois sous l'angle de biens numériques dont il s'agit de régir la succession ?

Nous illustrerons cette tension avec l'évolution du droit français en la matière.

EN FRANCE : DE LA JURISPRUDENCE A LA LOI

Le droit français se saisit diversement de ces données, à travers la notion de vie privée ou encore de données à caractère personnel sans toutefois parvenir encore à construire un régime global des données en ligne (Castex 2016).

En France, c'est d'abord le Code civil qui encadre le respect de la vie privée en disposant dans son article 9 que « Chacun a droit au respect de sa vie privée ». Cette disposition peut de prime abord sembler pertinente pour appuyer un régime de gestion, par un individu, de ses éternités numériques : données que l'on souhaite voir de son vivant disparaître, comme données qui survivent à son décès. Un obstacle majeur remet toutefois rapidement en cause cette première appréciation. Le droit au respect de la vie privée ne trouve

17 L'article 228 de la Loi C de 2012 portant Code pénal (2012. évi C. törvény a Büntető Törv énykönyvről) institue un « délit d'impiété » (*kegyeletsértés*) à la mémoire du défunt

application que du vivant d'un individu, ce droit étant un droit de la personnalité, rattaché à la personne et qui disparaît avec elle[18], il est non transmissible. Il permet toutefois de gérer l'existence et la persistance de certains éléments numériques qui porteraient atteinte à la vie privée d'un individu de son vivant. De même, le droit au respect de la vie privée ne peut être invoqué, du vivant de la personne, par des proches incidemment concernés par la publication d'une information.

Une autre difficulté réside dans l'appréciation du standard juridique que constitue la notion de vie privée et son rapport au droit à la protection des données personnelles. Une jurisprudence abondante (Antin et Brossolet, 1999) permet d'en évaluer les contours même si plusieurs conceptions coexistent. La vie privée peut d'abord être envisagée comme l'espace réservé nécessaire à la construction d'un individu et à son épanouissement. Une part de la jurisprudence lie vie privée et intimité, à travers la notion d'atteinte à l'intimité de la vie privée (Antin et Brossolet, 1999). Or l'intimité est un critère à la fois rigide et relatif (Castex 2016). Chaque individu, en un temps donné, en un espace donné, dans un contexte personnel donné, pourra avoir sa propre idée de ce qui lui est intime au sens de ce qu'il considère devoir ne pas être livré aux espaces numériques. Cette conception peut évoluer au cours de son existence ; c'est justement une des approches du droit à l'oubli qui vise à pouvoir revenir sur certaines données publiées. Par ailleurs, si l'on interprète la vie privée comme un espace réservé et un droit à être laissé tranquille, ce qui est le cas dans le paradigme de la vie privée partagé par la coalition de cause dont fait partie la CNIL, la notion peut être élargie au-delà des données à caractère intime : ainsi s'applique-t-elle aux loisirs (Antin & Brossolet 1999)[19]. Il en est de même du secret des correspondances, protection pénale spécifique du courrier comme du courrier électronique qui cesse en sa forme avec le décès de l'intéressé (Castex 2017).

[18] « Le droit au respect de la vie privé prend fin à la mort de son titulaire », Cass. civ. 1, 14 décembre 1999, 97-15.756**,** *SA Editions Plon v Mitterand.*V. également Cass. civ. 2, 8 juillet 2004, n° 03-13.260 et Cass. civ. 1, 15 fév ; 2005, n° 03-18302.

[19] V. Cass. civ. 2, 10 mars 2004, n° 01-15.322.

Après la mort de la personne, les héritiers peuvent éventuellement invoquer, pour eux-mêmes et au nom de leurs propres droits de la personnalité, une atteinte à leur vie privée, à leur réputation et à leur honneur, découlant de mentions faites de leur ascendant. C'est une forme de protection par ricochet. La jurisprudence fait parfois une application extensive du droit au respect de la vie privée, acceptant une notion se rapprochant d'une « vie privée de la famille » qui permettrait de faire perdurer, au-delà de la mort et pour quelque temps, la vie privée d'un individu. Ainsi certaines information seraient considérées comme pouvant également atteindre la vie privée de l'entourage familial[20]. Ce temps révolu, la vie privée s'efface peu à peu pour entrer dans l'histoire. Une appréhension générale des données numériques et de leur transmission ne pourra que difficilement, en tout état de cause, passer par le droit personnel de l'article 9 du Code civil. Le droit français mobilise également le concept de dignité humaine[21] pour protéger le corps du défunt et notamment ses représentations. Ce droit au respect du corps ne cesse pas avec la mort et s'étend aux restes ou aux cendres. La jurisprudence a ainsi pu retenir que « les proches d'une personne peuvent s'opposer à la reproduction de son image après son décès, dès lors qu'ils en éprouvent un préjudice personnel en raison d'une atteinte à la mémoire ou au respect dû au mort »[22].

La loi du 6 janvier 1978 « relative à l'informatique, aux fichiers et aux libertés »[23] a alors progressivement introduit un cadre protecteur concernant les données à caractère personnel. Elle introduit en effet l'idée d'un droit de l'individu sur des données directement ou indirectement identificatrices. L'article 40 ancien[24] de la loi prévoyait déjà une possibilité d'actions pour l'intéressé de son vivant, sur les données ainsi utilisées par un tiers. L'intéressé peut exiger du responsable d'un traitement que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel le concernant « qui sont inexactes, incomplètes, équivoques, périmées, ou dont

[20] CA Paris, 17 déc. 1973. Et CA Paris 21 déc. 1977.
[21] Article 16 et s. du Code civil
[22] Cass. civ. 1, 1er juillet 2010, 09-15.479
[23] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dite loi Informatique et libertés.
[24] Avant l'entrée en vigueur de la loi pour une République numérique

la collecte, l'utilisation, la communication ou la conservation est interdite »[25]. Le responsable du traitement doit alors « justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées » [26]. L'effacement numérique peut ici porter sur « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».

L'article 63 de la loi pour une République numérique est venu ajouter un paragraphe I à l'article 40 de la loi Informatique et liberté, notamment en vue de prendre en compte la notion de « mort numérique »[27].

Les droits sur les données à caractère personnel restent tout d'abord par défaut des droits *intuitu personae* puisque selon cet article « les droits ouverts à la présente section s'éteignent au décès de leur titulaire ». Ils peuvent toutefois être provisoirement maintenus dans les cas et conditions énumérées par la loi.

L'article 40-1-II prévoit tout d'abord que tout individu pourra « définir directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières ».

Les directives générales sont définies comme couvrant « l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés » (art. 40-1 de la loi informatique et libertés). Quant aux directives particulières, il s'agit « des traitements de données à caractère personnel mentionnées par ces directives » (tel service numérique par exemple). Elles sont enregistrées auprès de chaque responsable de traitement concerné. Ces directives spécifiques doivent faire l'objet d'un consentement spécifique de la personne concernée et ne peuvent pas résulter de la seule acceptation des conditions générales d'utilisation

[25] Art. 40 al. 1 ancien de la loi Informatique et libertés.
[26] Art. 40 al. 2 ancien de la loi Informatique et libertés.
[27] Projet de loi pour une République numérique, art. 32-4, version adoptée en première lecture par l'Assemblée nationale.

(CGU). En effet le sort des données peut échapper à la volonté par l'application des CGU, souvent standardisées, qui excluent la transmissibilité à cause de mort.
La loi a ici voulu parer à l'existence d'une multitude de CGU , souvent complexes[28], variables dans le temps en donnant préséance aux directives énoncées par la personne concernée sur les dites conditions d'utilisation.

Ces deux types de directives poursuivent le même but, à savoir permettre à la personne de stipuler comment seront exercés ses droits après son décès sur ses données personnelles. Ces directives sont modifiables et révocables à tout moment. Un registre unique des directives générales doit voir le jour à l'image du fichier national des testaments. Le décret d'application est attendu.

Une personne de confiance « a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés » (art. 40-I). Cependant, à défaut de personne désignée dans les directives, les héritiers ont qualité pour en prendre connaissance au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés. De même, en l'absence de directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés mais uniquement dans certains cas, à savoir dans la mesure nécessaire au règlement d'une liquidation ou encore au partage de la succession. Une exception s'applique aux souvenirs de famille, concept civiliste qui attache des droits spécifiques aux souvenirs en raison d'une prédominance de la valeur sentimentale sur la valeur patrimoniale. Ainsi, d'une photo, d'un courrier électronique. Si l'héritier peut accéder au journal intime ou aux lettres missives, biens matériels de son parent (Castex 2017), le peut-il pour leur équivalent numérique ?

Autrement dit, les droits sur les données concernées continuent de s'éteindre à la mort de la personne qui en était détentrice ou productrice. Ces dispositions ne permettent donc pas de reconnaître, par défaut, les droits des héritiers sur

[28] En France, une réflexion sur les CGU est menée par la DGCCRF sous l'angle des clauses abusives, et par l'ISOC sous l'angle de leur simplification.

ces données.

Cette frontière entre une forme de subsistance de la volonté d'inspiration personnaliste et le droit des successions – droit réaliste - suppose la présence d'acteurs habituellement absents du champ de la protection des données personnelles à l'exemple des notaires. Enfin, comme nous le verrons, la question de savoir si nous devons considérer le sort des données *post-mortem* sous l'angle de la vie privée fait débat.

Demeure également la question des droits sur des données qui ne seraient pas à caractère personnel mais seulement constitutifs de l'activité en ligne de l'utilisateur décédé : par exemple des bibliothèques en ligne de vidéos, de musiques, de livres (Castex 2011).

L'ensemble de ces limites pourrait nous inviter à rechercher, en dehors de la protection de la vie privée et des données à caractère personnel stricto sensu, un cadre plus général pour les éternités numériques. Le Conseil d'État[29] s'éloigne pour le moment d'une telle solution qui passerait par la propriété interrogeant cependant la dimension patrimoniale des données numériques (Banta, 2014 et Peres, 2016) au-delà des données à caractère personnel.

ANALYSE DE LA CONTROVERSE AUTOUR DU NOUVEL ARTICLE 40-1 DE LA LOI INFORMATIQUE ET LIBERTES FRANÇAISE

Comme nous l'avons vu, la loi pour une République numérique du 7 octobre 2016, crée par son article 63 un nouvel article 40-1 dans la loi Informatique et Libertés. Cette disposition a fait l'objet de débats en commission, tant à l'Assemblée nationale (Belot, 2016) qu'au Sénat (Frassa, 2016). Elle a également suscité des réactions et des contributions pendant une consultation publique en ligne sur le site web www.republique-numerique.fr. En analysant les compte-rendus des débats en commission, sur le site web de

[29] Voir : Conseil d'Etat, *Le numérique et les droits fondamentaux*, Etude annuelle 2014, La Documentation française

la consultation republique-numerique.fr, nous avons cherché à déterminer à quel référentiel obéissaient les dispositions du nouvel article 40-1, et quelles étaient les controverses qu'il cristallisait.

Toute politique, comme le rappelle Pierre Müller, « passe par la définition d'objectifs […] qui vont eux-mêmes être définis à partir d'une représentation du problème, de ses conséquences, et des solutions envisageables pour le résoudre » (Müller, 2011:54). C'est ce qu'il appelle la « fonction cognitive » (Müller, 2011:55) de l'action publique. Cet ensemble de représentations constituent ce qu'il appelle un « référentiel ». D'autres politistes ont également étudié les représentations sous-jacentes aux politiques publiques, notamment Paul Sabatier (Sabatier, 1998), qui étudie les coalitions d'acteurs cherchant à influencer les effets d'une politique publique pour déterminer les différentes représentations en circulation.

Selon Paul Sabatier, mener une étude sur des coalitions d'acteurs suppose d'abord l'existence d'un sous-système de politique publique stable sur une période de dix ans (Sabatier, 1998). Ce qui n'est évidemment pas le cas pour les politiques relatives à la mort numérique, qui, de fait, relèvent comme nous le verrons d'une intersection entre les politiques publiques en matière de droit successoral et celles relatives à la protection des données personnelles.

Comme nous l'avons vu dans un paragraphe précédent, les politiques publiques de protection des données se structurent en Europe autour d'un paradigme de la vie privée partagé par une communautés d'acteurs organisés en réseau transgouvernemental et comprenant les autorités nationales de protection des données, comme la CNIL.

Cependant, en France, les principes juridiques de la protection des données obéissant à ce référentiel ne s'appliquent théoriquement qu'aux données relatives à des personnes vivantes. Dès lors qu'une donnée se réfère directement ou indirectement à une personne décédée, la loi Informatique et Libertés (sauf son nouvel article 40-1) et, bientôt, le RGPD, ne s'appliquent plus.

Pourtant, Christophe-André Frassa, rapporteur au nom de la Commission des lois du Sénat du projet de loi pour une République numérique, note dans son rapport que :

> « En principe, à la mort de la personne, les données à caractère personnel qui permettent de l'identifier ne devraient plus être conservées : l'article 36 de la loi informatique et libertés interdit en effet que lesdites données soient conservées au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées. Or, l'immense majorité des services en ligne sont destinés à des personnes vivantes, pour rendre compte de leur activité, leur proposer des prestations ou les mettre en relation avec d'autres personnes : autant de finalités qui n'ont plus de sens une fois que la personne concernée est décédée » (Frassa, 2016, pp. 155-156)

Or, cette interprétation est juridiquement erronée, puisque de toutes façons, une fois que la personne est décédée, la loi informatique et libertés n'a plus lieu de s'appliquer aux données auxquelles la personne est reliée.

La CNIL et le Conseil supérieur du notariat sont les deux organismes ayant influencé le processus d'adoption de l'article sur la mort numérique dans la loi pour une République numérique, et qui sont cités dans les rapports parlementaires.

L'extension de la logique informatique et libertés, et donc de la logique inhérente au référentiel du paradigme de la vie privée est notamment l'œuvre de la CNIL. En effet, selon l'avis de la CNIL sur le projet de loi, cité dans le rapport de Luc Belot, rapporteur au nom de la Commission des lois de l'Assemblée nationale du projet, l'article relatif à la mort numérique « répond à un besoin de clarifier le devenir des données personnelles des personnes décédées » et « constitue le prolongement naturel du droit de disposer librement de ses données » (Belot, 2016, pp. 459-460, citant : CNIL, 2015)

Or, ce droit à la libre-disposition de ses données personnelles, aussi appelé droit à l'auto-détermination informationnelle (*informationelle Selbstbestimmung*) est bien un concept, inspiré du droit constitutionnel

allemand[30] (Kilian, 2010), propre à l'univers de la protection des données.

Sur le site de la consultation en ligne « République Numérique.fr », bon nombre de commentaires abondaient dans le sens d'une protection de la vie privée des défunts. Ainsi, selon l'utilisateur « alice bachelier » :

> « La famille n'est pas "propriétaire" de ses membres, chaque membre est libre d'informer ou non, de donner accès ou non. La mort n'est pas une raison valable pour mettre son nez dans la vie d'un autre, lien familial ou pas. Les ados décédés ont aussi droit à leur intimité. Ce qu'on a choisi de garder privé et perso de notre vivant, doit le rester ! [...] »[31]

Cette idée se fonde notamment sur l'idée de l'attente raisonnable que les personnes avaient de leur vivant que leurs données personnelles resteraient couvertes par le secret y compris après leur mort. Ainsi, selon Luc Belot, un mauvais encadrement de la transmission des données personnelles d'un défunt « pourrait conduire […] à révéler aux proches de la personne décédée des informations à caractère personnel ou professionnel qu'elle avait souhaité tenir secrètes » (Belot, 2016, p. 462).

C'est pour cela que la Commission des lois de l'Assemblée a adopté des amendements visant à renforcer l'encadrement la transmission des droits relatifs aux données personnelles du défunt. Alors que dans sa version d'origine, le texte prévoyait, en l'absence de directives laissées par le défunt, la transmission des droits d'accès aux héritiers du défunt, il a été décidé, sur proposition du gouvernement lui-même, et « suivant des préoccupations

---

30 Ce droit a été consacré par l'arrêt « Volkszählungsurteil » du 15 décembre 1983 du Tribunal constitutionnel fédéral de la République fédérale d'Allemagne (BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83)

31 Page http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees, sous l'onglet « Arguments »

formulées par la CNIL » (Belot, 2016, p. 463), de poser le principe d'une intransmissibilité des droits d'accès après le décès du titulaire lorsque ce dernier n'a pas laissé de directive.

Ce principe connaît cependant une exception, inspirée, elle, d'une logique successorale, protégeant cette fois non pas l'intérêt du défunt en matière de vie privée mais celui des héritiers. Elle leur permet d'accéder aux données de la personne décédée lorsqu'elles sont utiles à la liquidation et au partage de la succession. Ce référentiel successoral était poussé par le Conseil supérieur du notariat.

Cette organisation chercha notamment à se positionner pour que les notaires deviennent les « tiers de confiance » auprès desquels les particuliers pourront déposer les directives relatives au sort de leurs données après la mort. Leur intervention contribua aux éléments du nouvel article 40-1 de la loi informatique et libertés inspiré du droit des successions. Ainsi, leur contribution disponible publiquement sur le site « République numérique.fr » rejette la logique d'une extension du référentiel du paradigme de la vie privée à la mort numérique :

> « […] « La protection de la vie privée ». [...] tant le renvoi à la notion de « vie privée en ligne » que la formule de l'article 20 occultent les grands principes régissant les droits de la personnalité et notamment l'article 9 du Code civil sur le respect à la vie privée. Les droits de la personnalité sont en effet intransmissibles aux héritiers (car ils s'éteignent avec la personne du défunt). Le droit à l'oubli, le droit à la vie privée et les droits sur les données personnelles sont des droits personnels (et non des droits réels).
>
> S'agissant du droit au respect de la vie privée, la jurisprudence de la Cour de cassation, en application de l'article 9 précité, considère que le droit au respect de la vie privée s'éteint à la mort de son titulaire ; les héritiers peuvent uniquement défendre leur propre droit à la vie

privée. […] »[32]

Ils ont également, avec succès, obtenu que les personnes soient libres de la forme des directives relatives à leurs données personnelles, en se basant sur la tradition de la liberté de rédaction testamentaire :

> « […] La forme des directives. L'article 20 II prévoit que les directives sont rédigées selon un modèle dont le contenu est fixé par décret en Conseil d'Etat. A notre sens, il serait plus opportun de laisser à la personne le choix de la forme de ses directives. L'usage d'un imprimé Cerfa ou d'un modèle de clauses empêcherait le particulier de formuler ses directives autrement, notamment dans un testament qu'il soit rédigé de sa main ou établi devant notaire. […] »[33]

Et ils ont critiqué ce qu'ils ont perçu comme l'invention d'une exception au fonctionnement classique des successions, qui aboutirait à déconnecter la succession numérique du reste de la succession :

> « […] Comme le souligne l'exposé sommaire du projet de loi, il s'agit de réfléchir à ce qu'il advient des données numériques appartenant à une personne à son décès.
>
> Le premier réflexe pour répondre à cette question est de raisonner par rapport au champ connu de la dévolution successorale des biens d'un

32 Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Contribution du Conseil supérieur du notariat : observations sur la mort numérique (art. 20) » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/contribution-du-conseil-superieur-du-notariat-observations-sur-la-mort-numerique-art-20

33 Idem

défunt. [...]

Or le monde numérique contient des données et des informations détenues par le défunt ou relatives à lui qui n'ont pas particulièrement de valeur économique ou patrimoniale.

Néanmoins, il nous semble que le sort des données personnelles doive relever du droit des successions et précisément de la succession anomale, comme c'est le cas en matière de propriété littéraire et artistique pour la transmission du droit moral de l'auteur ou en cas de transmission d'un souvenir de famille ou d'une sépulture de famille.

Dans sa version initiale, l'article 20 nous semble être déconnecté des problématiques du droit des successions. Il ne répond pas à la question de savoir si les données se transmettent par voie successorale, notamment par voie anomale. Il ne définit pas qui est l'héritier, ne fixe pas de rang de priorité et ne règle pas l'hypothèse d'éventuels conflits en cas de pluralité de successibles.

A notre sens, le présent dispositif ne doit pas être le prétexte d'une évolution du droit des successions ; il doit au contraire y correspondre afin d'éviter toute difficulté dans son application. Autrement dit, les conséquences de la mort numérique devraient être assimilées dans la mesure du possible à celles de la mort physique. […] »[34]

La commission des lois du Sénat, majoritairement de l'opposition de droite au gouvernement socialiste de l'époque, a adopté une position moins favorable à l'extension du paradigme de la vie privée, se rapprochant de l'approche du Conseil supérieur du notariat, mêlée à des éléments visant à protéger l'intérêt mémoriel du défunt.

Comme le rappelle en introduction le rapporteur du Sénat : « la

34 http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/contribution-du-conseil-superieur-du-notariat-observations-sur-la-mort-numerique-art-20

réforme proposée par le Gouvernement croise deux approches différentes : celle du droit des successions et celle du droit des données personnelles » (Frassa, 2016, p. 162). Mais il atteint mal l'équilibre entre les deux. Pour Christophe-André Frassa, l'approche adoptée par la Commission des lois de l'Assemblée aboutit en effet à une « absolutisation du droit au respect de la vie privée » et à une « césure […] entre le monde numérique et le monde physique » (Frassa, 2016, p. 164).

Il reprend en cela à son compte des conclusions de Cécile Pérès qui assimile les données du défunt à un patrimoine numérique, à des souvenirs de famille, auquel les héritiers et les proches devraient avoir par défaut le droit d'accéder :

> « nul ne songerait à interdire aux héritiers de lire le journal intime du défunt ou ses lettres missives, de regarder ses albums de photographies ou, plus largement, de conserver ses souvenirs personnels au nom de la vie privée de celui qui n'est plus. Dans le monde physique, il appartient à chacun de prendre la précaution de faire disparaître de son vivant les supports de ses secrets » (Pérès, 2016, cité par Frassa, 2016, p. 165).

Plus loin, le rapport de Christophe-André Frassa, reprenant là encore des arguments de Cécile Pérès, cite explicitement en modèle le droit états-unien de patrimonialisation des données *post-mortem*, qui permettrait de ne pas créer de rupture entre les successions physiques et les successions numériques.

Le référentiel de la patrimonialisation de ces données dans une logique successorale, qui sous-tend le droit états-uniens en contraste avec les tendances européennes en la matière, a donc lui aussi joué un rôle significatif dans les débats parlementaires et pré-parlementaires qui ont précédé son adoption, au côté d'une logique assimilant ces données au référentiel du paradigme de la vie privée. Le texte finalement adopté en France, bien qu'il penche largement en faveur de ce dernier, suivant en cela les préférences de

la commission des lois de l'Assemblée nationale et de la CNIL, n'est de ce fait pas non plus tout à fait exempt de traces d'une vision successorale et patrimoniale des données *post-mortem*.

Conclusion

En matière de réglementation du sort des données *post-mortem*, deux logiques s'opposent.

La première, qui prévalait originellement aux Etats-Unis était celle de considérer ces données comme un patrimoine à transmettre. Cette logique protégeait avant tout les intérêts des héritiers et des proches, facilitant l'accès au patrimoine numérique laissé par la personne. Elle a aujourd'hui partiellement reculé face au lobbying d'entreprises du numérique, qui au nom de la vie privée des défunts gardent ainsi dans un grand nombre de cas le contrôle sur le contenu des données *post-mortem*, la liberté testamentaire pouvant remettre en cause ce contrôle. Cependant, le droit américain des données *post-mortem*, tout en restreignant l'accès aux données personnelles des défunts au nom de la vie privée, reste insérée dans une logique de droit successoral.

La seconde, qui prévaut, assez largement en Europe et notamment en France sous l'influence des autorités de protection des données reprenant là - fait rare - les arguments des GAFA en faveur d'une vie privée après la mort, étend la logique de la protection des données personnelles aux données *post-mortem*. Cette logique protège essentiellement les intérêts du défunt en matière de vie privée, et peut être couplée – c'est le cas notamment en Hongrie – à la protection par le code pénal de sa mémoire. Cependant, la possibilité pour le défunt de prévoir un accès possible à ses données dans des directives n'est pas sans rappeler la liberté testamentaire.

En France, un nouvel article dans la loi informatique et libertés régit désormais le devenir des données *post-mortem*. Les débats parlementaires

autour de cet article ont reproduit la ligne de clivage entre ces deux logiques qui s'étaient déjà opposées auparavant aux Etats-Unis. La commission des lois de l'Assemblée nationale, se rangeant à l'avis de la CNIL, avait adopté une ligne étendant la portée du paradigme de la vie privée aux données *post-mortem* tandis que celle du Sénat, reprenant des arguments avancés par le Conseil supérieur des notaires, souhaitait amender le texte dans une direction plus inspirée de la logique successorale.

Le résultat en est un rattachement qui n'est cependant que partiel des données *post-mortem* aux politiques publiques de protection des données. Car y compris dans la version défendue par l'Assemblée nationale et dans le texte final, une place est laissée à la logique testamentaire. En effet, chacun est libre de définir par des directives un droit d'accès des héritiers et des proches à son patrimoine numérique. Et les notaires se sont très tôt positionnés pour être les tiers de confiance auprès de qui de telles directives pourraient être enregistrées. Leur rôle précis, et donc l'influence qu'ils pourront avoir sur la mise en œuvre concrète de ces nouvelles dispositions, dépendra d'un décret d'application qui peut encore apporter des modifications au placement du curseur oscillant entre la logique successorale et la logique du paradigme de la vie privée.

Quoi qu'il en soit, l'article 40-1 de la loi informatique et libertés continuera à s'appliquer avec l'entrée en vigueur d'un RGPD qui n'inclut pas les données *post-portem* dans son champ d'application. Or, cet article interdit, en l'absence de directives contraires, à quiconque d'accéder aux données personnelles d'un défunt pour un motif autre que celui de régler des questions liées à la succession ou d'accéder à des souvenirs de famille, à condition d'avoir connaissance au préalable de la nature de ces données. Dans cette hypothèse, dans une affaire similaire à celle de la mère berlinoise cherchant à accéder aux conversations de sa fille sur les réseaux sociaux pour déterminer si sa mort était un accident ou avait pu être un suicide, il est probable qu'un juge français soit amené lui aussi à lui refuser l'accès à ces données, puisque cet accès n'est pas utile pour régler une succession.

Ce cas peut dès lors servir d'illustration pour méditer la prise de position de l'Avocat général Michal Bobek de la Cour de justice de l'Union européenne, qui, dans son avis dans l'affaire « Rigas Satiksme » avait écrit :

> « […] le risque est de donner une interprétation trop large à ces règles [de protection des données personnelles]. Cela pourrait conduire à leur application également dans des situations dans lesquelles le lien avec l'objectif est quelque peu ténu et discutable. Une application trop large et, dans un certain sens, « absolue » pourrait aussi aboutir à discréditer l'idée de départ qui était très importante en soi et légitime » (Bobek, 2017, pt. 96)

Enfin, au-delà de la question de la vie privée, se pose également une question de philosophie sur le rapport à la mort. Le droit des données post-mortem doit-il défendre les intérêts des morts, ou bien ceux des vivants ? La question ne semble aujourd'hui pas tout à fait tranchée.

BIBLIOGRAPHIE

ANTIN (d'), A., BROSSOLET, L. (1999), « Le domaine de la vie privée et sa délimitation jurisprudentielle », Legicom 1999/4, n°20, p. 154.

AMERICAN LAW INSTITUTE, (1977), *Restatement of the law, second, torts*, St. Paul, Minnesota:American Law Institute Publishers

BANTA N. M., « Inherit the Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets at Death » 83 *Fordham Law Review* pp.799 et s.

BENNETT C.J., RAAB C.D., (2003), *The Governance of Privacy. Policy Instruments in Global Perspective*, Aldershot, Ashgate.

BOBEK, M. (2017). Conclusions de l'avocat général Michal Bobek présentées le 26 janvier 2017. Aff. C-13/16 « Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde contre Rīgas pašvaldības SIA « Rīgas satiksme » ». Document ECLI:EU:C:2017:43

BOURDELOIE H. (2015), « Usages des dispositifs socionumériques et communication avec les morts », *Questions de communication*, 28, p. 101-126.

CARDON D. (2010), *La Démocratie Internet. Promesses et limites*, Paris, Le Seuil, 112 p.

CASTEX L. (2011), « Bibliothèque numérique et gratuité », dans MBONGO, Pascal (dir.), *Le prix de la culture - La gratuité au prisme du droit et de l'économie*, Paris, Mare et Martin

CASTEX L. (2016), « Les éternités numériques. Un essai d'analyse prospective », *Revue Lamy droit de l'immatériel*, n° 126, pp. 49-54

CASTEX L. (2017), « Secret des correspondances en ligne, dans le sillon des lettres missives », *Revue Lamy droit de l'immatériel*, n° 137, pp. 46-54

DELEUZE G. (1990), « Post-scriptum sur les sociétés de contrôle », dans *Pourparlers*, Paris, Les éditions de Minuit, p. 240-247.

DE WAAL, M. J. (2007), « A Comparative Overview. » In REID, K., DE WAAL, M. J. et ZIMMERMANN, R. (dir.) *Exploring the law of Succession: Studies National, Historical and Comparative*, Edimbourg, Edinburgh University Press, pp. 1–27.

DU TOIT, F. (2000), « The Limits Imposed Upon Freedom of Testation by the Boni Mores: Lessons from Common Law and Civil Law (Continental) Legal Systems. » *Stellenbosch Law Review* 77, pp. 58–384.

EDWARDS, L. & HARBINJA, E. (2013), 'What Happens to My Facebook Profile When I Die?': Legal Issues Around Transmission of Digital Assets on Death' in Maciel, C. & Pereira, V. (eds.). *Digital Legacy and Interaction: Post-Mortem Issues*. (Springer, 2013) p. 115-144

EDWARDS, L and HARBINJA, E, (2013b) 'Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World' *Cardozo Arts & Entertainment Law Journal* 32(1) p. 83-129

FOUCAULT M. (1975), *Surveiller et punir. Naissance de la prison*, Paris, Gallimard.

GEORGES, F. et JULLIARD, V., (2014) « La construction de l'identité numérique, le cas des pages dédiées aux défunts sur Facebook », *Actes du 21ème congrès de la Société Française des Sciences de l'Information et de la Communication*, 4-6 juin 2014, Université du Sud Toulon Var. Disponible en ligne : http://sfsic2014.sciencesconf.org/30582/document (ressource consultée le 19 octobre 2017)

GEORGES, F., JULLIARD, V. (2016), « Profilopraxie et apposition des stigmates de la mort: comment les proches transforment-ils la page Facebook d'un défunt pour la postérité ? ». *Linguas e Instrumentos Lingüisticos*, 37, pp. 231-255

GONZALEZ FUSTER G. (2014), « Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection », *Birkbeck Law Review*, *2*, 2, p. 263-278.

GROUPE DE TRAVAIL DE L'ARTICLE 29 (G29), *Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets*, Groupe de travail de l'Article 29, Bruxelles, 16 septembre 2014. Disponible en ligne : http://ec.europa.eu/justice/data-protection/article- 29/documentation/opinion-recommendation/files/2014/wp223_fr.pdf (ressource consultée le 19 octobre 2017)

HARBINJA, E. (2017) 'Post-mortem Privacy 2.0: Theory, law and technology' *International Review of Law, Computers & Technology*. 31(1) 26-42

HONDIUS F.W. (1975), *Emerging data protection in Europe*, Amsterdam, Pays-Bas, Pays multiples, Elsevier, ix+282 p.

HOUSE OF LORDS, Select Committee on the European Communities (1992), *Report on the Protection of Personal Data*

HUET, J. ; DREYER,E., (2011), *Droit de la communication numérique*, LGDJ

HUSTINX, J.P. (2013). « EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation ». Papier rédigé sur la base d'un cours donné à l'Institut universitaire européen entre le 1er et le 12 février 2013. Disponible en ligne sur le site du Contrôleur européen de la protection des données : https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf (ressource consultée le 19 octobre 2017)

KILIAN W., (2010), « Germany », dans RULE J.B., GREENLEAF G. (dirs.), *Global privacy protection: the first*

generation, Cheltenham, Edward Elgar, p. 80-106.

LANZING M., (2016), « The transparent self », *Ethics and Information Technology*, volume 18 issue 1, p. 9-16.

LAW COMMISSION (2017). *Making a will. Consultation Paper 231*. Document disponible en-ligne (consulté le 31 octobre 2017) : https://s3-euwest-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2017/07/Making-awill-consultation.pdf

LOPEZ, A. B. (2016), 'Posthumous Privacy, Decedent Intent, and Post-mortem Access to Digital Assets' 24 George Mason Law Review 183

MILL J.S., (1989), *On liberty ; with The subjection of women ; and chapters on socialism*, COLLINI S. (dir.), Cambridge [England] ; New York, Cambridge University Press (Cambridge texts in the history of political thought), 289 p.

NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, Drafting Committee on Fiduciary Access to Digital Assets, 'Fiduciary Access to Digital Assets Act' (February 15-16, 2013 Drafting Committee Meeting)
http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2013feb7_FADA_MtgDraft_Styled.pdf

NEMZETI ADATVÉDELMI ÉS INFORMÁCIÓSZABADSÁG HATÓSÁG (NAIH). (2015), *A Nemzeti Adatvédelmi és Információszabadság Hatóság ajánlása az online adatok halál utáni sorsáról.*

NEWMAN A. (2008), *Protectors of Privacy. Regulating Personal Data in the Global Economy*, Ithaca, Cornell University Press.

OCDE (1974), *Questions d'ordre politique soulevées par la protection des données et des libertés individuelles, principes et perspectives. Compte-rendu du séminaire 24-26 juin 1974*, Paris, OCDE (Etudes d'informatique).

ORWELL G. (1949), *Nineteen Eighty-Four (1984)*, London, Secker & Warburg.

PERES, Cécile. (2016), « Les données à caractère personnel et la mort. Observations relatives au projet de loi pour une République numérique », *Rec. Dalloz* , 2016.90

PROSSER W. (1960), « Privacy », *California Law Review*, *48*, 3, p. 383.

ROCHELANDET F. (2010), *Économie des données personnelles et de la vie privée*, Paris, Découverte.

SABATIER P.A. (1998), « The Advocacy Coalition Framework: revisions and relevance for Europe », *Journal of European Public Policy*, 5:1, p. 98-130.

SEYFFARTH M. (2017), « Datenschutz gegen Moral », *DIE WELT*, 1 juin 2017.

SIMON B. (2002), « The Return of Panopticism: Supervision, Subjection and the New Surveillance », *Surveillance & Society*, *3*, 1.

SOLOVE, D.J. (2006), « A Brief History of Information Privacy Law » in *Proskauer on Privacy*, PLI (2006).

SÓLYOM L. (1988), « Egy új szabadságjog: az információszabadság », *Valóság*, 31, p. 14-34.

WARREN S.D., BRANDEIS L.D. (1890), « The Right to Privacy », *Harvard Law Review*, *4*, 5, p. 193-220.

WEINER, M. M. (2015), « Opposition to the Uniform Fiduciary Access to Digital Assets Act », *The National Law Review*, 21 juillet : https://www.natlawreview.com/article/opposition-to-uniform-fiduciary-access-to-digital-assets-act

YOUNGER K. (1972), *Report of the committee on privacy. Chairman: Kenneth Younger. Presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by command of Her Majesty, July 1972.*, London, H.M.S.O.

CONSEIL D'ETAT. (1970), « Les conséquences du développement de l'informatique sur les libertés publiques et sur les décisions administratives », *Rapport annuel 1969-1970*, Paris, Conseil d'Etat.

Corpus de documents utilisés dans l'analyse des controverses sur l'article 40-1 de la loi informatique et libertés

BELOT, Luc. (2016), *Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, après engagement de la procédure accélérée, sur le projet de loi (n° 3318) pour une République numérique*. Rapport n° 3399. Ve République, XIVe législature. Rapport enregistré à la Présidence de l'Assemblée nationale le 15 janvier 2016. Disponible en ligne : http://www.assemblee-nationale.fr/14/pdf/rapports/r3399.pdf (ressource consultée le 18 octobre 2017)

Commission nationale de l'informatique et des libertés (CNIL), Délibération n° 2015-414 du 19 novembre 2015 portant avis sur un projet de loi pour une République numérique. Disponible en ligne : https://www.cnil.fr/sites/default/files/typo/document/D2015-414-PJLNumerique.pdf (ressource consultée le 18 octobre 2017)

FRASSA, Christophe-André. (2016), *Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale après engagement de la procédure accélérée, pour une* République numérique. Rapport enregistré à la Présidence du Sénat le 6 avril 2016. Rapport n° 534, session ordinaire de 2015-2016. Disponible en ligne : http://www.senat.fr/rap/l15-534-1/l15-534-11.pdf (ressource consultée le 18 octobre 2017)

Webographie des pages consultées sur le site « République numérique.fr » (pages consultées le 19 octobre 2017) :

- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees
- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Observations sur la mort numérique (contribution du Master 2 DC2EN) » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/observations-sur-la-mort-numerique
- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Informer les personne de la communication de données personnelles les concernants, et qu'elles peuvent s'y opposer. » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/informer-les-personne-de-la-communication-de-donnees-personnelles-les-concernants-et-qu-elles-peuvent-s-y-opposer
- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Enregistrement des directives auprès d'un notaire » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/enregistrement-des-directives-aupres-d-un-notaire
- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Clarification de l'article - Pas de directive générale possible - Instauration d'un régime post mortem par défaut? » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/clarification-de-l-article-pas-de-directive-generale-possible-instauration-d-un-regime-post-mortem-par-defaut
- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort

numérique - Contribution du Conseil supérieur du notariat : observations sur la mort numérique (art. 20) » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/contribution-du-conseil-superieur-du-notariat-observations-sur-la-mort-numerique-art-20

- Page « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Obliger le service visé à suivre les directives. » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/obliger-le-service-vise-a-suivre-les-directives

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Enregistrement des directives du traitement des données personnelles par un tiers » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/enregistrement-des-directives-du-traitement-des-donnees-personnelles-par-un-tiers

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - GRATUITE DU SERVICE » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/gratuite-du-service

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Orthographe : l'internet » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/orthographe-l-internet

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Tous les héritiers chargés de faire respecter les directives? » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/tous-les-heritiers-charges-de-faire-respecter-les-directives

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Forte adhérence de cet article avec d'autres (droit à l'oubli - portabilité) » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/forte-adherence-de-cet-article-avec-d-autres-droit-a-l-oubli-portabilite

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Droit de préemption de l'état ? » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/droit-de-preemption-de-l-etat

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - don numerique » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/don-numerique

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Mort numérique et droits immatériels » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/mort-numerique-et-droits-immateriels

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Modifications générales » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-

20-personnes-decedees/versions/modifications-generales

- Page : « République Numérique - Projet de loi pour une République numérique - Consultation - Article 20 - Mort numérique - Enregistrement des directives auprès de la CNIL » : http://www.republique-numerique.fr/projects/projet-de-loi-numerique/consultation/consultation/opinions/section-1-protection-des-donnees-a-caractere-personnel/article-20-personnes-decedees/versions/enregistrement-des-directives-aupres-de-la-cnil