FACULTÉ DES SCIENCES JURIDIQUES, POLITIQUES ET SOCIALES

MÉMOIRE DE RECHERCHE
MASTER 2 DROIT PUBLIC GÉNÉRAL ET
CONTENTIEUX PUBLICS

TRANSPARENCE DES ALGORITHMES DES POUVOIRS PUBLICS

Par Inès Mimouna BELKASMIOUI

Sous la direction de Monsieur le Professeur Aymeric POTTEAU

ANNÉE UNIVERSITAIRE 2017/2018

Remerciements

Je remercie le Professeur Aymeric Potteau pour avoir accepté d'encadrer ce mémoire de recherche avec patience et bienveillance.

Je remercie également mes parents pour leur soutien moral tout au long de mes études de Droit.

Sommaire

Liste des abréviations

AJDA	Actualité juridique Droit administratif
API	*Application Programming Interface*
CADA	Commission d'accès aux documents administratifs
CESDH	Convention européenne de sauvegarde des droits de l'homme
CNIL	Commission nationale de l'informatique et des libertés
CNNum	Conseil national du numérique
CPI	Code de la propriété intellectuelle
CRPA	Code des relations entre le public et l'administration
EUPL	*European Union Public License*
IFSA	Institut français des sciences administratives
PGO	Partenariat pour un gouvernement ouvert
RGPD	Règlement général sur la protection des données

Introduction

L'année 2018 a été le théâtre d'un vent de contestation contre la mise en place de la nouvelle plate-forme d'admission dans l'enseignement supérieur Parcoursup, qui est venue remplacer l'ancienne plate-forme Admission PostBac. En effet, outre la contestation de la mise en place d'une sélection à l'Université, il a été reproché à la nouvelle plate-forme l'opacité de l'algorithme[1]. Finalement, la veille de la phase d'admission des candidats, qui a débuté le 22 mai 2018, et à l'initiative de la ministre de l'Enseignement supérieur, de la Recherche et de l'Innovation, Frédérique Vidal, est publié le « code informatique des algorithmes » de Parcoursup[2]. Pour la ministre, « la publication du code permettra à chacun de vérifier que le fonctionnement de la plate-forme est conforme au droit. Elle favorisera également la pleine compréhension des mécanismes de la nouvelle procédure d'entrée dans l'enseignement supérieur »[3]. Consécutivement à la publication du code source de Parcoursup, le secrétaire d'État en charge du Numérique, Mounir Mahjoubi, a déclaré sur son compte Twitter que l'engagement du gouvernement était de garantir la transparence des algorithmes publics[4]. Ainsi, la mise en place de Parcoursup a donc également alimenté le débat plus général de la transparence des algorithmes des pouvoirs publics.

Le dictionnaire français/anglais de l'informatique définit l'algorithme comme « un ensemble ordonné et fini de règles déterminées servant à résoudre un problème »[5]. Il faut savoir que la notion d'algorithme est à distinguer de celle de programme

1 LE NEVÉ Soazig. « Parcoursup : ouverture des inscriptions sous haute tension ». L*eMonde.fr,* 22 janvier 2018. Disponible sur : https://www.lemonde.fr/campus/article/2018/01/22/parcoursup-ouverture-des-inscriptions-sous-haute-tension_5245273_4401467.html [consulté le 26/08/2018]

2 VIDAL Frédérique. « Parcoursup : publication du code informatique des algorithmes ». [communiqué]. Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, 21 mai 2018. Disponible sur : http://m.enseignementsup-recherche.gouv.fr/cid130453/parcoursup-publication-du-code-informatique-des-algorithmes.html [consulté le 26/08/2018]

3 *Ibid.*

4 MAHJOUBI Mounir (@mounir). « Avec @VidalFrederique, on l'a dit, on le fait ! Aujourd'hui nous rendons public 100% du code source de #Parcoursup et sa documentation scientifique. Notre engagement : garantir la transparence des algorithmes publics ». Twitter, 21 mai 2018, https://twitter.com/mounir/status/998524796307587072 [consulté le 26/08/2018]

5 LAFARGUE France. *Dictionnaire français/anglais de l'informatique. AFNOR,* 2003. Algorithme

informatique car, comme l'explique l'informaticien et mathématicien Donald Knuth, les algorithmes sont des concepts qui ont une existence propre et distincte de tout langage de programmation[6]. En effet, l'algorithme est une méthode abstraite de résolution d'un problème[7] et celle-ci peut être concrétisée de différentes façons, que ce soit dans un langage de programmation, dans un langage mathématique, dans la langue française, etc[8]. Le programme informatique se distingue donc de l'algorithme car il constitue la concrétisation de ce dernier dans un langage de programmation[9]. Aussi, un même algorithme peut être traduit en une multitude de programmes différents[10], de la même manière qu'une même histoire peut être traduite en une multitude de langues différentes. Le logiciel, quant à lui, constitue le regroupement d'un ensemble de programmes informatiques[11].

Donald Knuth admet qu'il est difficile aujourd'hui d'imaginer un algorithme qui ne serait pas définit dans un langage de programmation[12], c'est pourquoi généralement lorsqu'il est fait référence aux algorithmes, il est question de programmes informatiques. Dans le titre de ce mémoire, l'expression *algorithme* est préférée à celle de *programme informatique,* afin d'inclure toutes les formes de traductions d'algorithmes auxquelles les pouvoirs publics peuvent avoir recours, aujourd'hui et dans le futur. Néanmoins, les pouvoirs publics n'ayant recours aujourd'hui qu'à des algorithmes sous forme de programmes informatiques, les deux notions, telles qu'abordées dans ce mémoire, peuvent être considérées à l'heure actuelle comme synonymes.

---

6 KNUTH Donald. *Selected papers on computer science*. Center for the Study of Language and Information, 1996. p. 1

7 *Ibid.*

8 MODESTE Simon. *Enseigner l'algorithme pour quoi ? Quelles nouvelles questions pour les mathématiques ? Quels apports pour l'apprentissage de la preuve ?.* GRAVIER Sylvain (dir. De Recherche). Thèse de doctorat. Mathématiques-informatique. Université de Grenoble, 2012. p. 24

9 KNUTH Donald. *Op. cit.* p. 1

10 *Ibid.*

11 LILEN Henri. *Dictionnaire informatique et numérique.* Paris : Editions First-Gründ, 2011. Logiciel

12 KNUTH Donald. *Op. cit.* p. 1

Comme le constate le professeur Jean-Bernard Auby, le « tsunami de la transformation numérique »[13] n'a pas épargné les pouvoirs publics et cette numérisation de l'action publique s'explique notamment par le besoin de traiter une quantité de données en accroissement constant[14]. En effet, pour fonder leurs décisions, les pouvoirs publics ont besoin de traiter ces données mais elles ne peuvent plus le faire par le biais de leurs méthodes de traitement traditionnel en raison de l'énormité de leur quantité ; elles sont donc contraintes de recourir à des algorithmes afin de maîtriser cette complexité[15].

En France cette administration numérique s'est construite en plusieurs étapes[16]. A la fin des années 1990, elle a d'abord consisté en la communication d'informations (ex : Legifrance.gouv.fr), puis en la numérisation de formulaires[17] pour aujourd'hui « toucher en profondeur un nombre croissant de services publics »[18]. Ainsi, en plus de permettre un abaissement des coûts de l'administration, la numérisation a permis de faire évoluer l'administration vers « une dimension de plate-forme, sur laquelle les citoyens et les services publics interagissent »[19].

L'idée que l'action des pouvoirs publics doit être publique et non plus secrète est fort ancienne[20]. Ainsi, le philosophe Bentham expliquait, dans son projet de code constitutionnel, que les députés devaient s'engager à respecter dans leurs discours « la plus grande transparence et, donc, la plus grande simplicité possible »[21]. Néanmoins, Bentham parlait ici de publicité et non pas de la transparence[22]. Il était ainsi question au départ de publicité de l'action de l'administration et celle-ci « a donné

13 AUBY Jean-Bernard. « Le droit administratif face aux défis du numérique ». *AJDA,* 2018. p. 835
14 *Ibid.*
15 *Ibid.*
16 « Développement de l'administration électronique : où en est-on ? ». *Vie-publique.fr,* 7 avril 2005. Disponible sur http://www.vie-publique.fr/actualite/dossier/administration-electronique-2005/developpement-administration-electronique-ou-est-on.html [consulté le 27/08/2018]
17 *Ibid.*
18 ALGAN Yann, Maya BACACHE-BEAUVALLE, PERROT Anne. « Administration numérique », *Notes du conseil d'analyse économique*, 2016/7 (n° 34). p. 2
19 *Ibid.*
20 DENOIX DE SAINT MARC Renaud. « La transparence : vertus et limites ». *In :* IFSA, CADA. *Transparence et secret. Colloque pour le XXVe anniversaire de la loi du 17 juillet 1978 sur l'accès aux documents administratifs.* Paris : La documentation française, 2004. p. 11

lieu à l'élaboration du régime juridique des mesures de publicité des décisions administratives »[23]. L'idée d'une transparence des données publiques est en revanche plus récente[24] et a connu en France, ces dernières années, un important essor[25]. Elle est d'abord consacrée dans la loi du 17 juillet 1978 qui institue une liberté d'accès, pour le public, aux documents administratifs[26]. Puis cette dernière a depuis été modifiée de nombreuses fois, et inclut depuis 2005, la réutilisation des informations publiques[27]. L'ouverture des données publiques est concernée par une multitude de dispositions – se sont ajoutés à la loi de 1978 de nombreux textes, comme la loi pour une République numérique[28] – et ces dernières ont été codifiées dans le Code des relations entre le public et l'administration[29]. Dans ce contexte de politique d'ouverture des données publiques, pourquoi cette dernière doit-elle inclure la transparence des algorithmes des pouvoirs publics et comment cette transparence est-elle assurée ?

21 BENTHAM Jeremy. *Constitutional Code II, The Works of Jeremy Bentham.* Vol 9. p. 203. *Cité par :* ZOLLER Elizabeth. « Transparence et démocatie : généalogie d'un succès ». *In :* GUGLIELMI Gilles (dir.), ZOLLER Elizabeth (dir.). *Transparence, démocratie et gouvernance citoyenne. Colloque international des 23 et 24 mai 2014.* Paris : Editions Panthéon-Assas, 2014. p. 13

22 ZOLLER Elizabeth. « Transparence et démocatie : généalogie d'un succès ». *In :* GUGLIELMI Gilles (dir.), ZOLLER Elizabeth (dir.). *Op. cit.* p. 13

23 DENOIX DE SAINT MARC Renaud. *Op. cit.* p. 11

24 DENOIX DE SAINT MARC Renaud. *Op. cit.*. p. 11

25 CHEVALLIER Jacques. « Le droit français et la question des données publiques ». *In :* BOURCIER Danièle (dir.), DE FILIPPI Primavera (dir.). Open Data & Big Data: *Nouveaux défis pour la vie privée.* Editions mare&martin, 2016. p. 29

26 Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, JORF du 18 juillet 1978, p. 2851

27 Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, JORF n°131 du 7 juin 2005. p. 10022. Texte n°13

28 CLUZEL-METAYER Lucie. « Le Code face aux données ». *In :* KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Lectures critiques du Code des relations entre le public et l'administration.* LGDJ, 2018. p. 182

29 Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, JORF n°0248 du 25 octobre 2015, p. 19872. Texte n° 2 ; Décret n° 2015-1342 du 23 octobre 2015 relatif aux dispositions réglementaires du code des relations entre le public et l'administration (Décrets en Conseil d'Etat et en conseil des ministres, décrets en Conseil d'Etat et décrets), JORF n°0248 du 25 octobre 2015, p. 19895. Texte n° 3

Dans la première partie de ce mémoire, il sera démontré pourquoi la transparence des algorithmes des pouvoirs publics est nécessaire. En effet, les pouvoirs publics sont amenés aujourd'hui à utiliser des algorithmes dans plusieurs domaines ce qui peut présenter des risques pour l'exercice des droits et libertés fondamentaux, surtout dans les cas particuliers des décisions algorithmiques et du vote électronique. Dans la seconde partie de ce mémoire, seront étudiés les différents outils auxquels les pouvoirs publics peuvent recourir pour assurer cette transparence.

Partie 1 : Une nécessaire transparence des algorithmes des pouvoirs publics en raison des risques potentiels d'atteinte à des droits et libertés fondamentaux

La transparence des algorithmes des pouvoirs publics est nécessaire car leur recours peut présenter des risques d'atteinte à des droits et libertés fondamentaux. Ici, sont étudiés particulièrement les décisions prises sur le fondement d'algorithme (Section 1), et le vote électronique (Section 2).

Section 1 : Le cas des décisions prises par les pouvoirs publics sur le fondement d'un algorithme

Les pouvoirs publics peuvent être amenés à recourir à des algorithmes pour prendre des décisions, or, comme l'a entre autres rappelé le Conseil d'État dans son étude annuelle de 2014 sur le numérique et les droits fondamentaux, les algorithmes ne sont, par nature, ni objectifs, ni infaillibles (§1), et peuvent ainsi être sources de risques pour l'exercice des libertés(§2).

§1) Des décisions prises sur le fondement d'algorithmes qui ne sont ni infaillibles, ni objectifs, par nature

Il est courant de penser que les algorithmes sont infaillibles et objectifs[30]. Harry Surden explique ainsi que les technologies ont cette « aura d'objectivité et de neutralité »[31] car elles sont automatiques et non humaines, la subjectivité étant

30 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n°65. Paris : La documentation française, 2014. p. 234

31 SURDEN Harry. « Values Embedded in Legal Artificial Intelligence ». *U of Colorado Law Legal Studies Research Paper*, n°17-17, 15 mars 2017. p. 3

associée à l'humain. En effet, lorsqu'elle prend une décision, une personne peut être amenée à naturellement préférer certaines valeurs par rapport à d'autres, à être influencée par ses émotions, par ses préjugés, alors que la décision formée par une machine apparaît être à première vue le résultat d'une série de calculs et d'automatismes[32].

Mais, en réalité, les algorithmes ne sont pas objectifs car ils sont conçus par des humains qui, lors de cette conception, sont amenés à faire un certain nombre de choix, qui sont donc subjectifs, et intégrés dans l'algorithme[33]. Ainsi, le développeur d'une technologie détermine les fonctionnalités de celle-ci, ses limites, la manière dont les données seront analysées, la manière dont l'utilisateur interagira avec la machine par le biais de son interface, etc[34]. Et de la même manière qu'une personne qui prend une décision est plus ou moins influencée par son environnement et ses émotions, une personne sera influencée plus ou moins de la même manière lorsqu'elle sera amenée à concevoir des algorithmes.

Aussi, même dans l'hypothèse où l'algorithme serait conçu d'une manière objective, il peut néanmoins produire des résultats biaisés[35]. C'est le cas surtout des algorithmes d'apprentissage qui peuvent être amené à « apprendre » à partir de données collectées dans la société, qui contiennent des inégalités, exclusions et autres formes de discriminations et qui seront reproduites dans les résultats produits par l'algorithme, comme l'expliquent les auteurs Barocas et Selbst[36].

Un certain nombre de pouvoirs publics ont rappelé ainsi qu'il était faux de croire en l'objectivité et l'infaillibilité des technologies.

---

32 SURDEN Harry. « Values Embedded in Legal Artificial Intelligence ». *U of Colorado Law Legal Studies Research Paper*, n°17-17, 15 mars 2017. p. 3

33 BURREL Jenna. « How the machine ' thinks ' : Understanding opacity in machine learning algorithms ». Big Data & Society, Volume 3, Issue 1, January-June 2016. p. 3

34 SURDEN Harry. *Op. cit.* p. 1

35 GOODMAN Bryce, FLAYMAN Seth. « European Union regulations on algorithmic decision-making and a ' right to explanation ' ». *AI Magazine*, Vol 38, No 3, 2017. p. 3

36 BAROCAS Solon, SELBST Andrew. « Big Data's Disparate Impact ». *California Law Review,* n°104. *Cité par :* GOODMAN Bryce, FLAYMAN Seth. *Op. cit.* p. 3

Ainsi, en décembre 2017, la CNIL a souligné la subjectivité des algorithmes dans son rapport « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle ». En effet, la commission explique que tout algorithme est biaisé dans « , dans la mesure où il est toujours le reflet – à travers son paramétrage et ses critères de fonctionnement, ou à travers les données d'apprentissage qui lui ont été fournies – d'un système de valeurs et de choix de société »[37].

La « Commission Informatique et libertés » – une commission créée à la suite de l'affaire « S.A.F.A.R.I » et chargée de proposer une réglementation relative à l'utilisation informatique des données[38] – dans son rapport de de 1975, dit « rapport Tricot », précise que les algorithmes ne sont pas infaillibles non plus. En effet, la Commission explique qu'en plus des simples erreurs que l'ordinateur peut commettre et qu'il peut être programmé à repérer, l'ordinateur peut également commettre des erreurs, « des raisonnements faux qui peuvent paraître corrects du point de vue logique […] devant lesquels l'ordinateur n'aura aucune capacité d'étonnement »[39] – c'est à dire que l'ordinateur peut produire des résultats faux qui ne seront pas considérés par l'ordinateur comme erronés et ainsi seront considérés comme vrais par l'utilisateur. Pour la commission, la réputation selon laquelle « l'ordinateur ne se trompe pas »[40] a de quoi inquiéter car elle peut amener à entourer d'une autorité des résultats faux sous prétexte qu'un ordinateur est réputé infaillible[41].

37 Commission nationale de l'informatique et des libertés. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle.Synthèse du débat public anumé pa la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique,* Décembre 2017. p. 31

38 « Création de la Commission nationale de l'informatique et des libertés (CNIL) ». Disponible sur : https://www.gouvernement.fr/partage/9870-creation-de-la-commission-nationale-de-l-informatique-et-des-libertes-cnil [consulté le 23/08/2018]

39 Commission Informatique et libertés. *Rapport de la Commission informatique et libertés.* Paris : La documentation française, 1975. p. 15

40 *Ibid.*

41 *Ibid.*

Aussi, le Conseil d'État dans son rapport public annuel de 2014 sur le numérique et les droits fondamentaux constate également qu'aujourd'hui est encore attribué aux résultats des algorithmes une supposée infaillibilité et objectivité[42]. Le Conseil d'État reprend les affirmations du rapport Tricot selon lesquelles il est faux de croire que « l'ordinateur ne se trompe pas » et rappelle qu'un algorithme peut produire des résultats biaisés – en raison de la présence de biais dans les données collectées – et des corrélations qui ne correspondent à aucun lien de causalité[43].

Cette subjectivité et faillibilité des algorithmes pose problème car, comme l'explique Lawrence Lessig dans son article « Code is Law », ce sont ces derniers qui vont déterminer comment la vie privée est protégée, comment le discours est censuré, si l'accès à l'information est général ou s'il dépend de la zone géographique où l'utilisateur se situe, etc[44], si bien que ces choix subjectifs opérés par le concepteur, et intégrés dans les algorithmes, peuvent avoir pour effet de promouvoir certaines valeurs par rapport à d'autres[45]. Certaines fonctionnalités peuvent également avoir été intégrées de manière involontaire, tout en ayant également pour effet de promouvoir certaines valeurs par rapport à d'autres, mais cette fois à l'insu du concepteur et parfois d'une manière difficilement détectable[46]. Cela pose problème notamment lorsque ces derniers transposent des règles de droit[47] puisque les pouvoirs publics peuvent recourir à des algorithmes susceptibles de présenter des risques pour l'exercice des libertés.

42 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n°65. Paris : La documentation française, 2014. p. 234-235
43 *Ibid.* p. 235
44 LESSIG Lawrence. « Code is law. On liberty in Cyberspace ». *Harvard Magazine*, janvier 2000. p. 1. Disponible sur : https://harvardmagazine.com/2000/01/code-is-law-html [consulté le 22/08/2018]
45 SURDEN Harry. « Values Embedded in Legal Artificial Intelligence ». *U of Colorado Law Legal Studies Research Paper*, n°17-17, 15 mars 2017. p. 2
46 *Ibid.* p. 3
47 *Ibid.* p. 2

§2) Faillibilité et subjectivité qui sont sources de risques pour les libertés

Le premier risque soulevé par cette subjectivité et faillibilité est que les pouvoirs publics peuvent être amenés à recourir des algorithmes qui produisent des résultats qui mettent en œuvre des discriminations illicites[48]. Ce fut le cas du logiciel COMPAS, logiciel de prédiction de la récidive utilisé dans les tribunaux états-uniens, qui s'est révélé produire des scores racistes, d'après les révélations du site internet ProPublica, puisqu'il attribuait, à tort, un fort taux de récidive à l'encontre des personnes noires[49].

Cela s'explique par le fait que le concepteur d'un algorithme, lorsqu'il transpose des règles de droit dans ce dernier, intègre sa propre interprétation de la norme dans l'algorithme, si bien qu'il peut être amené à modifier volontairement ou maladroitement la portée de celle-ci[50] et ainsi concevoir volontairement ou involontairement un algorithme qui porte atteinte au libertés des personnes concernées.

Aussi, comme expliqué dans la partie précédente, dans le cas spécifique des algorithmes d'apprentissage, ces discriminations peuvent être mises en œuvre indépendamment de la volonté ou de la qualité de la transposition de la norme par le concepteur de l'algorithme. En effet, l'algorithme d'apprentissage peut reproduire des discriminations qui étaient initialement présentes dans les données et sur lesquelles il s'est basé pour construire sa logique.

---

48 Commission nationale de l'informatique et des libertés. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle.Synthèse du débat public anumé pa la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique,* Décembre 2017. p. 31

49 ANGWIN Julia, LARSON Jeff, MATTU Surya, KIRCHNER Lauren. « Machine Bias. There's software used across the country to predict future criminals. And it's biased against black ». *Propublica.org,* 23 mai 2016. Disponible sur : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [consulté le 25/08/2018]

50 BOURCIER Danièle, DE FILIPPI Primavera. « Les algorithmes sont-ils devenus le langage ordinaire de l'administration ? ». *In :* KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Lectures critiques du Code des relations entre le public et l'administration*. LGDJ, 2018. p. 207

La transposition de règles juridiques dans un algorithme peut également soulever un problème d'évolution du droit[51]. En effet, la norme a cette particularité de pouvoir être interprétée de multiples façons, d'être flexible, si bien que le rôle du juge, par exemple, est d'adapter l'application de la norme en prenant en considération tout un tas d'éléments, dont les circonstances particulières de l'espèce[52]. En revanche, lorsque la norme est transposée dans l'algorithme, l'interprétation du concepteur de l'algorithme devient figée dans ce dernier[53], puisque l'algorithme constitue une suite finie et non ambiguë d'instructions[54]. La norme ainsi mise en œuvre par l'algorithme perd de sa flexibilité et de sa capacité à s'adapter à des circonstances imprévues[55]. Cela entraîne non seulement le risque de limiter l'application de la norme à des cas prédéfinis – et ainsi d'empêcher l'adaptation de la norme à des situations nouvelles ou imprévues – mais cela entraîne également le risque d'appliquer la norme à des situations auxquelles elle n'était pas sensée s'appliquer[56].

51 Maître Louis DEGOS. *Cité par :* SILGUY Stéphanie De. « Doit-on se méfier davantage des algorithmes ? ». *Revue Lamy Droit civil*, n°146, 1er mars 2017. p. 5. Disponible sur : www.lamyline.fr [consulté le 16/02/2018].

52 SURDEN Harry. « Values Embedded in Legal Artificial Intelligence ». *U of Colorado Law Legal Studies Research Paper*, n°17-17, 15 mars 2017. p. 5

53 *Ibid.*

54 Commission nationale de l'informatique et des libertés. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle.Synthèse du débat public anumé pa la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique,* Décembre 2017. p. 5

55 SURDEN Harry, GENESERETH Michael, LOGUE Bret. « Representational Complexity in Law ». *Proceedings of 11th International Conference on Artificial Intelligence and Law*, 2007. p. 193-194. *Cité par :* BOURCIER Danièle, DE FILIPPI Primavera. « Les algorithmes sont-ils devenus le langage ordinaire de l'administration ? ». *In :* KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Op. cit.* p. 200

56 BOURCIER Danièle, DE FILIPPI Primavera. *Op. cit*. p. 200

En raison des risques qu'ils présentent pour l'exercice des libertés, certains pouvoirs publics ont ainsi rappelé que la transparence des algorithmes est primordiale. En effet, la transparence permet non seulement de vérifier que l'algorithme met correctement en œuvre les règles de droit qui sont transposées, mais a également pour but de permettre la contestation de sa logique[57].

Le Conseil d'État dans son rapport public annuel de 2014 sur le numérique et les droits fondamentaux a souligné que les algorithmes en général présentaient trois sources de risques pour l'exercice des libertés à savoir « l'enfermement de l'internaute dans une personnalisation dont il n'est pas maître, la confiance abusive dans les résultats d'algorithmes supposés objectifs et infaillibles, l'apparition de problèmes nouveaux d'équité par l'exploitation de plus en plus fine des données personnelles »[58]. En raison de ces risques d'atteinte aux libertés, le Conseil d'État souligne que, afin de donner aux individus les garanties appropriées face aux algorithmes prédictifs qui peuvent être utilisés pour prendre des décisions à leur égard, quatre objectifs doivent être poursuivis : « assurer l'effectivité de l'intervention humaine dans la prise de décision, veiller à la non discrimination, mettre en place des garanties de procédure et de transparence, développer le contrôle des résultats produits par les algorithmes »[59]. Pour le Conseil d'État, lorsqu'une personne est affectée par une décision en partie fondée sur un algorithme, elle devrait avoir le droit d'être informée des données utilisées par l'algorithme, afin de s'assurer de leur véracité, mais également d'être informé sur la logique de l'algorithme, tout ceci afin de lui permettre de faire valoir ses observations[60].

57 FOREST David. « La régulation des algorithmes, entre éthique et droit ». *Revue Lamy Droit de l'Immatériel*, n°137, 1er mai 2017. p. 7

58 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n°65. Paris : La documentation française, 2014. p. 234

59 *Ibid.* p. 237

60 *Ibid.* p. 301

De même, le Parlement européen, dans une résolution du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique, insiste sur le principe de transparence « de toute décision prise avec l'aide de l'intelligence artificielle qui est susceptible d'avoir une incidence importante sur la vie d'une ou de plusieurs personnes »[61]. Ainsi, il doit toujours être possible de traduire dans une forme humainement compréhensible les calculs d'un système d'intelligence artificielle et que ce dernier devrait être doté d'une « boite noire » contenant les données relatives aux opérations réalisées par le système, y compris les logiques de ce dernier[62].

Enfin, la Commission européenne explique également qu'en raison du fait que les algorithmes sont à la base de plus en plus de décisions concernant la vie quotidienne, la transparence de ces derniers est alors primordiale[63].

61 Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)). Point 12

62 *Ibid.*

63 Commission européenne. « Une approche européenne en matière d'intelligence artificielle ». *Questions et réponses.* Bruxelles, le 25 avril 2018

Section 2 : Le cas du vote électronique

Une élection est démocratique si lors de son déroulement ont été respectés les principes fondamentaux du droit électoral, leur respect étant exigé quel que soit la modalité de vote choisie. Il est donc exigé des systèmes de vote électronique qu'ils soient sécurisés, afin que ces principes soient garantis et respectés (§1) et cette sécurité des systèmes de vote électronique doit nécessairement s'accompagner de leur transparence (§2).

§1) L'exigence de la garantie des principes fondamentaux du droit électoral par des dispositifs de vote électronique sécurisés

Avec le développement des nouvelles technologies, est née la « promesse d'une nouvelle ère »[64] où la machine vient remplacer l'homme, synonyme de partialité, d'erreur et de tentatives de fraude[65]. En effet, le développement de l'informatique a permis l'apparition d'une nouvelle modalité de vote, qui s'ajoute aux procédures classique de vote en personne par bulletin papier ou de vote par correspondance postale : le vote électronique. Le vote électronique, qui est « un vote réalisé à l'aide de systèmes informatiques, […] un vote dématérialisé »[66], désigne deux modalités d'exercice du vote, tout deux impliquant un ordinateur et donc des algorithmes : le vote sur une machine à voter dans un bureau de vote et le vote à distance par Internet à partir de n'importe quel ordinateur[67].

64 KOUBI Geneviève. « Les machines à voter en questions… parlementaires ». *Revue du droit public,* n°1, Janvier 2014. p. 101. Disponible sur : https://www.lextenso.fr/ [consulté le 18/07/2018]

65 *Ibid.*

66 LE BOT Olivier. « Le vote électronique : modalités, potentialités, dangers ». *In :* LE BOT Olivier (dir.), ARLETTAZ Jordane (dir.). *La démocratie en un clic ? Réflexions autour de la notion d'e-démocratie. Actes du colloque de Nice – 16 novembre 2009.* Paris : L'Harmattan, 2010. p. 45

67 *Ibid.* p. 46

Présenté initialement comme une solution à la fraude électorale[68], le recours au vote électronique peut présenter plusieurs avantages. Tout d'abord, celui-ci peut réduire significativement les coûts d'organisation d'une élection, puisqu'il entraîne une réduction de la charge de travail des personnels ainsi que leur nombre[69]. Ces derniers n'ont plus besoin de mettre en place les urnes, les bulletins, enveloppes et les isoloirs puisque tout ces éléments peuvent être regroupés en une machine de vote[70]. Il peut entraîner également un gain de temps au dépouillement puisqu'il permet d'obtenir les résultats plus rapidement mais aussi, le processus étant automatisé, il permet d'effectuer plus facilement, rapidement et sans erreur, des procédures et des calculs complexes, comme les calculs de représentation proportionnelles[71].

Le vote électronique peut avoir également l'avantage d'être écologique, puisque les bulletins et les enveloppes papier sont remplacés par une machine[72], laquelle pouvant être réutilisée lors de plusieurs élections différentes. Aussi, le vote électronique, et spécifiquement le vote à distance par Internet, est vu comme une solution à la baisse de participation, et en particulier des jeunes citoyens, puisque ici le vote apparaît comme simplifié, plus spontané et confortable par rapport au vote papier qui implique un déplacement au bureau de vote[73].

---

68 GUGLIELMI Gilles. « Le vote électronique saisi par le droit : le cas français ». *In :* GUGLIELMI Gilles (dir.), IHL Olivier (dir.). Le vote électronique. LGDJ, 2015. p. 124

69 GICQUEL Jean-Eric. « Le vote électronique en France ». Petites affiches, n°68. p. 5. Disponible sur : https://www.lextenso.fr/ [consulté le 18/07/2018]

70 DOMPINER Nathalie. « Adopter ou abandonner les ordinateurs de vote ? Une focale locale sur les procédures démocratiques ». *In :* GUGLIELMI Gilles (dir.), IHL Olivier (dir.). *Le vote électronique.* LGDJ, 2015. p. 144

71 BIRCH Sarah, COCKSHOTT Paul, RENAUD Karen. « Putting Electronic Voting under the Microscope ». *The Political Quaterly,* vol. 85, n°2, April-June 2014. p. 188 Disponible sur : https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-923X.12071 [consulté le 17/07/2018]

72 LE BOT Olivier. « Le vote électronique : modalités, potentialités, dangers ». *In :* LE BOT Olivier (dir.), ARLETTAZ Jordane (dir.). *La démocratie en un clic ? Réflexions autour de la notion d'e-démocratie. Actes du colloque de Nice – 16 novembre 2009.* Paris : L'Harmattan, 2010. p. 55

73 BUCHSTEIN Hubertus. « Online Democracy, Is it Viable ? Is it Desirable ? Internet Voting and Normative Democratic Theory ». *In :* KERSTING Norbert, BALDERSHEIM Harald. *Electronic Voting and Democracy : A comparative Analysis.* Palgrave Macmillan, 2004. p. 45

Enfin, les contraintes économiques étant réduites et l'action de voter depuis son ordinateur personnel étant moins laborieuse, les citoyens peuvent être invités à se prononcer lors d'élections plus fréquentes. Ainsi, sans forcément passer d'une démocratie représentative à une démocratie participative, l'avènement du vote à distance par Internet rend possible une plus grande participation des citoyens à la vie publique et ainsi peut être conçu *a minima* comme un « correctif participatif à une démocratie représentative »[74].

C'est en raison de tous ces avantages que de nombreux États ont décidé de moderniser leurs élections en recourant au vote électronique lors de leurs élections politiques. Ainsi, en France, la loi du 10 mai 1969 est venue autoriser pour la première fois l'utilisation de machines à voter dans les bureaux de vote des communes[75]. Quant au vote à distance par Internet, il est possible pour l'élection des députés par les Français établis hors de France[76].

Néanmoins, et quant bien même le vote électronique peut présenter de nombreux avantages, la modernisation des modalités de vote ne doit pas se faire au détriment du respect des principes fondamentaux du droit électoral, à savoir le secret du vote et la sincérité du scrutin. Un scrutin sincère peut se définir comme étant « l'exact reflet de la volonté, exprimée par la majorité du corps électoral » et trouve son unité autour du respect des principes fondamentaux d'égalité, de liberté et de secret du vote[77], comme l'explique le professeur Richard Ghevontian. Quant au principe de secret du vote, il implique que doit être garanti à l'électeur la possibilité d'accomplir son vote de manière confidentielle, c'est à dire à l'abri des regards, et de manière anonyme, c'est à dire qu'il

74 LE BOT Olivier. « Le vote électronique : modalités, potentialités, dangers ». *In :* LE BOT Olivier (dir.), ARLETTAZ Jordane (dir.). *La démocratie en un clic ? Réflexions autour de la notion d'e-démocratie. Actes du colloque de Nice – 16 novembre 2009.* Paris : L'Harmattan, 2010. p. 57

75 Loi n°69-419 du 10 mai 1969 modifiant certaines dispositions du code électoral

76 Ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France

77 GHEVONTIAN Richard. « La notion de sincérité du scrutin ». Cahiers du Conseil Constitutionnel, n°13, Dossier : la sincérité du scrutin, Janvier 2003. Disponible sur : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-notion-de-sincerite-du-scrutin [consulté le : 3 août 2018]

n'est pas possible de le relier au suffrage qu'il a déposé[78]. Le secret du vote implique également que l'électeur ne puisse pas prouver son vote et éviter ainsi qu'il ne subisse des pressions lors du choix de son vote[79]. Le secret du vote est garanti à l'article 3 de la Constitution française qui dispose que « le suffrage […] est toujours universel, égal et secret »[80], à l'article 3 du Protocole additionnel à la Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales du 20 mars 1952 qui dispose que « les Hautes Parties contractantes s'engagent à organiser, à des intervalles raisonnables, des élections libres au scrutin secret »[81] et la Charte des droits fondamentaux de l'Union européenne dispose à l'article 39 que « Les membres du Parlement européen sont élus au suffrage universel direct, libre et secret »[82].

Ainsi, le déroulement d'une élection impliquant le respect et la garantie de principes fondamentaux, les instruments de vote électronique doivent obligatoirement être sécurisés ; la modernisation du processus et l'efficacité ne devant pas se faire au prix des droits fondamentaux des électeurs. En effet, un système de vote électronique qui n'aurait pas été convenablement sécurisé risque d'être dysfonctionnel et ainsi par exemple porter atteinte à la sincérité du scrutin en présentant des résultats erronés à l'issue du scrutin[83] ou en modifiant le vote de l'électeur à son insu[84].

La Commission nationale de l'Informatique et des libertés (CNIL) a notamment rappelé cette exigence de sécurité des dispositifs de vote électronique en 2003 dans une recommandation relative à la sécurité des systèmes de vote électronique, qui sera abrogée et remplacée par une recommandation de 2010. Dans cette recommandation,

78 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». *In :* FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie.* Paris : L'Harmattan, 2011. p. 86

79 ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». *Science et pseudo-Sciences,* n°320, avril 2017. Disponible sur : http://www.pseudo-sciences.org/spip.php?article2800 [consulté le 3 août 2018]

80 Constitution du 4 octobre 1958. Article 3

81 CESDH, Protocole additionnel. Article 3

82 Charte des droits fondamentaux de l'Union européenne. Article 39

83 ENGUEHARD Chantal. « Le vote électronique en France. Opaque et vérifiable ». *Legalis.net,* décembre 2006, n°4, p. 85

84 *ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». Science et pseudo-Sciences,* n°320, avril 2017

après avoir rappelé que le recours à des systèmes de vote électronique doit se faire dans le respect des principes fondamentaux du droit électoral, la CNIL a fixé un certain nombre de garanties qui doivent être respectées afin qu'un système de vote électronique puisse être considéré comme sécurisé. Ainsi, afin que le secret du vote soit protégé, doit être garantie la séparation des données nominatives des électeurs et des votes « par la mise en œuvre de procédés rendant impossible l'établissement d'un lien entre le nom de l'électeur et l'expression de son vote »[85]. Aussi, pour que soit garantie la sécurité du système de vote et la sécurité et la confidentialité des données personnelle, la CNIL recommande que les algorithmes de chiffrement et de signature électronique soient des algorithmes publics réputés forts[86]. Enfin, la CNIL recommande que les systèmes de vote électronique, la liste des candidats, la liste d'émargement et l'urne électronique fassent l'objet d'un scellement en recourant à des algorithmes publics réputés forts – le scellement étant « un procédé permettant de déceler toute modification du système »[87].

De même, le Conseil de l'Europe, dans une recommandation REC(2004)11 du 30 septembre 2004 sur les normes relatives au vote électronique, abrogée et remplacée par la recommandation CM/REC(2017)5 du 14 juin 2017, après avoir également rappelé que les systèmes de vote électronique doivent être conformes aux principes relatifs aux élections démocratiques, a défini un certain nombre de critères auxquels les États devraient se conformer afin de proposer aux électeurs des systèmes sécurisés. Le Conseil de l'Europe recommande ainsi, notamment, que le système de vote soit conçu de telle manière qu'il ne soit pas possible d'établir un lien entre le vote et l'électeur, qu'il assure la confidentialité des suffrages, que ces derniers soient scellés jusqu'au moment du dépouillement et que le système soit conçu de manière à empêcher de voter plusieurs fois.

85 CNIL. Délibération n° 03-036 du 1 juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, §I-2.

86 *Ibid.* §I-3 « Les sécurités informatiques »

87 CNIL. Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, §I-4 « Le scellement du dispositif de vote électronique »

Cette conformité du système de vote électronique aux exigences de sécurité peut être constatée par la délivrance d'un agrément. Ainsi, en France, les machines à voter doivent être un modèle agréé par arrêté du ministère de l'Intérieur[88]. Néanmoins, quant bien même il existerait une présomption irréfragable d'infaillibilité d'un système de vote électronique, ces mesures de sécurité doivent nécessairement s'accompagner de la transparence du système car non seulement la transparence permet de vérifier que le système est sécurisé mais elle permet également d'obtenir la confiance des électeurs[89].

§2) Une sécurité qui doit nécessairement être accompagnée d'une transparence des dispositifs de vote électronique

Tout d'abord, il est important de souligner que le vote par bulletin papier se caractérise par sa transparence tout au long de la procédure. En effet, sans passer par une personne tierce, les électeurs peuvent observer le déroulement du scrutin, tout au long de la journée[90]. Ils peuvent ainsi vérifier la présence d'isoloirs, que l'urne est transparente et vide au début du scrutin, que personne ne vient rajouter illicitement des bulletins dans cette dernière, que le dépouillement est public, que l'urne a été brassée avant d'être vidée, etc. La transparence permet ainsi aux électeurs de constater que le scrutin s'est bien déroulé et qu'aucune atteinte n'a été portée aux principes fondamentaux du droit électoral[91]. En revanche, si le système est opaque, les atteintes à ces principes sont indétectables.

88 Article L57-1 du code électoral

89 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». In : FOREY Elsa (dir.), GESLOT Christophe (dir.). Internet, machines à voter et démocratie. Paris : L'Harmattan, 2011. p.87

90 ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». Science et pseudo-Sciences, n°320, avril 2017. Disponible sur : http://www.pseudo-sciences.org/spip.php?article2800 [consulté le 3 août 2018]

91 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». *Op. cit.* p. 99

Si traditionnellement, l'élection par bulletin papier se caractérise par sa transparence, il est difficile alors de comprendre pourquoi l'ajout d'une nouvelle modalité de vote, en l'occurrence le vote électronique, s'accompagnerait de son opacité, quant bien même sa sécurité serait garantie. En effet, comme l'explique Chantal Enguehard, la promesse de sécurité d'un système de vote électronique ne peut justifier son opacité[92]. Tout d'abord parce qu'aujourd'hui un système ne peut pas être garanti comme étant absolument infaillible. En effet, il peut subir des dysfonctionnements divers qui peuvent avoir pour source une mauvaise conception ou une mauvaise manipulation[93]. Mais aussi, un système opaque empercherait la détection de manipulations frauduleuses, que celles ci soient internes, c'est-à-dire menées par les personnes impliquées dans l'organisation du vote, ou externes, c'est à dire menées par une personne extérieure à l'organisation du vote[94] qui aurait réussi à contourner les systèmes de sécurité ou exploité une faille de sécurité. La transparence permet donc de prévenir ou de constater ces dysfonctionnements, d'empêcher ou de constater les fraudes et de prouver devant le juge le mauvais déroulement du scrutin.

Mais surtout, Chantal Enguehard explique que quant bien même un système de vote pouvait être garanti comme étant totalement infaillible, cette garantie est sans intérêt si le système est opaque car l'électeur, ne pouvant vérifier l'effectivité de cette sécurité, n'y accordera pas sa confiance[95]. Les systèmes de vote électronique doivent donc nécessairement être transparent car cette dernière permet d'obtenir la confiance des électeurs, surtout que, par nature, le vote électronique nécessite une « confiance accrue de l'électeur »[96] puisque le système est moins transparent que le vote par bulletin papier. En effet, comparé au bulletin papier que l'électeur voit glisser dans l'urne transparente devant lui, l'électeur ne voit pas directement la série d'opérations et

92 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». In : FOREY Elsa (dir.), GESLOT Christophe (dir.). Internet, machines à voter et démocratie. Paris : L'Harmattan, 2011. p.100

93 *Ibid.* p. 96

94 *Ibid.* p. 98

95 *Ibid.*p. 100

96 GICQUEL Jean-Eric. « Le vote par Internet : une modalité électorale à aborder avec circonspection ». *La semaine juridique – Éditions administrations et collectivités territoriales,* n°31-35, 31 juillet 2006. p. 1093

calculs effectués par l'ordinateur au moment où il effectue son vote. En conséquence, un système de vote électronique opaque impliquerait que l'électeur lui accorde une confiance plus grande que celle qu'il ne lui accorde déjà, une confiance aveugle, exclusivement fondée sur l'assurance invérifiable que le système est sécurisé[97]. L'accord d'une telle confiance ne paraît pas réaliste, en raison notamment des nombreuses élections qui ont été marquées par des dysfonctionnements des systèmes de vote électronique[98]. Ainsi, en France, lors du premier tour de l'élection présidentielle de 2007, où certaines communes ont eu recours à des machines à voter, des écarts ont été constatés entre le nombre d'émergements constatés et le nombre de votes enregistrés sur les machines[99]. De même, en Belgique, à Schaerbeek, lors des élections législatives de 2003, un candidat avait recueilli plus de voix que le nombre de suffrages exprimés (un écart de 4096 voix)[100]. Enfin, aux États-Unis, aux élections présidentielles de 2004 ont été recensés près de 1000 incidents liés aux machines de votes[101]. Ainsi comme le souligne le Professeur Jean-Eric Gicquel, « on est encore loin du *zero fault system* »[102].

Certes, ces incidents ne sont pas récents et l'évolution des technologies est telle que les systèmes sont de plus en plus sécurisés aujourd'hui, néanmoins les électeurs restent conscients qu'un système infaillible n'existe pas et il n'est donc pas possible de croire que ces derniers consentiraient à y accorder une confiance absolue et aveugle. Or, comme le rappelle le Conseil de l'Europe, la confiance dans les systèmes de vote est nécessaire puisqu'elle influence de manière déterminante le niveau de participation et est un élément essentiel du système démocratique[103] ; la confiance dans le système

97 ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». Science et pseudo-Sciences, n°320, avril 2017. Disponible sur : http://www.pseudo-sciences.org/spip.php?article2800 [consulté le 3 août 2018]

98 ENGUEHARD Chantal. « Le vote électronique en France. Opaque et vérifiable ». *Legalis.net,* décembre 2006, n°4, p. 90

99 Rapport d'information de MM. Alain ANZIANI et Antoine LEFÈVRE, fait au nom de la commission des lois, n° 445 (2013-2014) - 9 avril 2014

100 *Ibid.*

101 GICQUEL Jean-Eric. « Le vote électronique en France ». Petites affiches, n°68. p. 5. Disponible sur : https://www.lextenso.fr/ [consulté le 18/07/2018]

102 *Ibid.*

et dans ses procédures est une source de légitimité démocratique[104]. Par conséquent, le système de vote électronique doit nécessairement être transparent, afin que l'électeur puisse lui accorder cette confiance essentielle.

103 Recommandation Rec(2004)11 du Comité des Ministres aux Etats membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (adoptée par le Comité des Ministres le 30 septembre 2004, lors de la 898e réunion des Délégués des Ministres). Exposé des motifs, point 55

104 BUCHSTEIN Hubertus. « Online Democracy, Is it Viable ? Is it Desirable ? Internet Voting and Normative Democratic Theory ». In : KERSTING Norbert, BALDERSHEIM Harald. Electronic Voting and Democracy : A comparative Analysis. Palgrave Macmillan, 2004. p. 49

Partie 2 : Outils de garantie de la transparence des algorithmes des pouvoirs publics

Il peut être contribué à la transparence des algorithmes des pouvoirs publics par la communication d'une diversité d'éléments à une diversité de destinataires et par une diversité de contributeurs (Section 1). Enfin, les pouvoirs publics peuvent garantir cette transparence en recourant à des instruments contraignants ou en privilégiant le recours à des licences dites ouvertes (Section 2).

Section 1 : Les éléments à prendre en compte lorsqu'est envisagée la transparence des algorithmes des pouvoirs publics

Il convient de relever qu'il existe une diversité d'éléments pouvant contribuer plus ou moins à la transparence des pouvoirs publics (§1), une diversité des destinataires de cette transparence et enfin une diversité de ses contributeurs (§2).

§1) Différents degrés de transparence des algorithmes des pouvoirs publics

Un certain nombre d'informations peuvent contribuer à la transparence d'un algorithme. En fonction des informations divulguées, celui-ci sera considéré comme plus ou moins transparent.

A) Types d'informations contribuant peu à la transparence d'un algorithme

Tout d'abord, l'intéressé peut simplement être informé que le pouvoir public fait usage d'un algorithme, que ce soit pour un usage interne ou pour prendre des décisions. Ainsi, par exemple, l'usager peut être informé que la décision dont il a fait

l'objet a été prise sur le fondement d'un algorithme et ainsi peut demander à l'administration plus d'informations sur cet algorithme, ou, si les normes en vigueur le permettent, demander une intervention humaine.

Le pouvoir public peut également publier une liste des algorithmes auxquels il a recours. Ainsi, le Conseil de l'Europe a recommandé que les autorités électorales publient une liste officielle des logiciels utilisés lors d'une élection électronique, avec leur version, leur date d'installation et une brève description. En effet, il explique que publier des descriptions des matériels et logiciels utilisés dans le cadre du vote électronique permettra aux groupes intéressés de vérifier par eux-mêmes que les systèmes utilisés correspondent à ceux certifiés par les autorités compétentes[105].

En réalité, publier une liste des algorithmes accompagnés de leur version contribue assez peu à la transparence. En effet, l'usager ne peut savoir comment se comporte cet algorithme, si il contient des failles de sécurité, s'il met en œuvre des discriminations, s'il contient des malveillances, etc. Tout au plus, il saura si le pouvoir public a recours à des algorithmes récents – sans que cela ne signifiasse nécessairement qu'ils soient conformes au droit, ou sécurisés. En effet, un algorithme à jour n'est pas nécessairement un algorithme sécurisé car des failles de sécurité, ou des dysfonctionnements, peuvent subsister ou apparaître, malgré ou avec les mises à jour. Ainsi, au début de l'année 2018, Intel a, par exemple, recommandé à ses utilisateurs de ne plus déployer leur mise à jour sur leur systèmes car celle-ci peut provoquer des redémarrages imprévus et d'autres comportements imprévisibles du système[106]. La mise à jour d'Intel a donc été ici source de dysfonctionnements plutôt que source de sécurité.

105Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique, point 31a)

106SHENOY Navin. « Root cause of reboot issue identified ; updates guidance for customers and partners ». Intel Newsroom, 22 janvier 2018. Disponible sur : https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/ [consulté le 20/08/2018] ; SHENOY Navin. « Intel security issue update : addressing reboot issues ». Intel Newsroom, 11 Janvier 2018. Disponible sur : https://newsroom.intel.com/news/intel-security-issue-update-addressing-reboot-issues/ [consulté le 20/08/2018]

En revanche, publier la liste des logiciels utilisés par le pouvoir public peut contribuer à la transparence si ces derniers ont déjà été rendus transparents par le concepteur, l'opacité ici ne résultant que du fait que l'usager ne connaissait pas le nom des logiciels auxquels recourait le pouvoir public. Ainsi, par exemple, le pouvoir public peut informer les usagers qu'il recourt au logiciel Apache pour ses serveurs et ainsi l'usager n'aura plus qu'à s'orienter vers le site internet du distributeur pour se procurer les codes sources et la documentation. Par contre, si le pouvoir public n'informe pas l'usager qu'il a recourt à ce logiciel, bien que ce dernier soit transparent, cette transparence ne jouera pour lui et le logiciel auquel le pouvoir public a recours pour ses serveurs restera donc opaque pour l'usager, car inconnu.

L'explication de l'algorithme n'est également pas suffisante pour en connaître toutes les fonctionnalités, pour contrôler qu'il fonctionne correctement et pour vérifier qu'il ne comprend aucune faille de sécurité ou malveillance. L'explication contribue tout au plus à rendre transparent l'objectif que poursuit le pouvoir public, lorsqu'il choisit de recourir à un algorithme particulier, et la manière dont il a l'intention de traiter des données. Mais l'explication ne suffit pas à contrôler la présence de failles, de malveillances ou d'erreurs. Aussi, avec une simple explication, il est impossible de vérifier que l'algorithme tel qu'il est mis en œuvre correspond à l'algorithme tel qu'il est décrit. La fourniture de l'explication de l'algorithme contribue donc assez peu à la transparence de ce dernier.

Pour un algorithme traduit en programme informatique, un élément décrit de manière exhaustive toutes les instructions de ce dernier : le code source. Permettre ainsi l'accès à celui-ci, selon les cas, peut contribuer à rendre entièrement transparent l'algorithme, ou peut être une contribution minimale à la transparence de l'algorithme.

B) Le code source : contribution minimale ou maximale à la transparence d'un algorithme

Comme expliqué dans l'introduction, un algorithme peut être exprimé de différentes façons, que ce soit dans un langage de programmation, dans un langage mathématique, dans la langue française, etc[107]. Ainsi, destiné à être exécuté par un ordinateur, le programme informatique est la concrétisation d'un algorithme dans un langage de programmation[108]. Le code source représente quant à lui l'ensemble des instructions d'un programme informatique, d'après la définition fournie par la Commission d'accès aux documents administratifs[109].

Avoir accès au code source peut présenter ainsi plusieurs intérêts. Tout d'abord, il permet de vérifier que l'algorithme effectue bien les tâches telles que le pouvoir public les a décrites, lorsqu'il a fournit des explications. En effet, l'algorithme étant une méthode abstraite et le programme sa réalisation concrète[110], il peut y avoir des différences, légères ou importantes, entre le programme tel qu'il a été imaginé et le programme tel qu'il est concrétisé, si l'algorithme a mal été traduit. Le code source étant un descriptif exhaustif de toutes les instructions du programme, il peut donc révéler ces différences ou encore des fonctionnalités que le pouvoir public n'a volontairement ou involontairement pas révélé, ou des dysfonctions qui n'avaient pas été décelées lors de l'exécution du programme. En revanche, si le code source n'est pas accessible, il est impossible de vérifier si les résultats produits par l'algorithme, tel qu'il est mis en œuvre, produit des résultats vrais, faux, loyaux ou non[111]. De plus, pour les algorithmes qui transposent des règles de droit, l'accès au code source permet de

107MODESTE Simon. *Op. cit.* p. 24

108KNUTH Donald. *Op. cit.* p. 2

109Commission d'accès aux documents administratifs, Avis n°20144578, séance du 8/01/2015, Direction générale des finances publiques (DGFIP) et Avis n°20161989, séance du 23/06/2016, Ministère de l'éducation nationale

110KNUTH Donald. *Op. cit.* p. 1-2

111SILGUY Stéphanie De. « Doit-on se méfier davantage des algorithmes ? ». Revue Lamy Droit civil, n°146, 1er mars 2017. p. 7

l'auditer et de vérifier ainsi que l'algorithme respecte bien les règles de droit qu'il est sensé implémenter[112]. L'accès au code source permet également d'assurer la sécurité du programme car il devient possible de l'analyser afin de détecter éventuellement des failles de sécurité et de les corriger : un programme dont le code source est public bénéficie ainsi d'une communauté et donc d'un plus grand nombre de personnes veillant à sa sécurité[113]. L'accès au code source permet également de détecter la présence de malveillances. Pour les algorithmes utilisés par l'administration pour prendre des décisions, rendre accessible le code source permet non seulement à l'usager de mieux comprendre comment les données sont traitées par l'administration[114], de comprendre le fonctionnement du programme, mais peut éventuellement aussi lui permettre de contribuer à celui-ci et de l'améliorer[115]. Ainsi, en avril 2016, la Direction générale des Finances publiques a été la première administration française a ouvrir le code source d'un de ses programmes, à savoir le code source du simulateur de calcul de l'impôt, ce qui a permis aux usagers de proposer des projets ayant pour objectif l'amélioration de la transparence et de l'efficacité de l'administration fiscale[116].

Le code source certes décrit de manière exhaustive toutes les instructions du programme et permet ainsi d'en connaître toutes les fonctionnalités, néanmoins celui-ci peut également être opaque. Son opacité peut découler de sa rédaction. En effet, il peut être rédigée de manière inintelligible, le rendant incompréhensible, même pour un programmeur expérimenté ; on parle alors de code impénétrable, ou de code obscur. La technique visant à rendre inintelligible un code source est appelée offuscation (*obfuscation* en anglais). L'offuscation consiste à transformer le code source afin de le

112BOURCIER Danièle, DE FILIPPI Primavera. « Les algorithmes sont-ils devenus le langage ordinaire de l'administration ? ». *In :* KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Op. cit.* p. 203

113FOUTEL Nathalie. « Licences libres en secteur industriel sensible : un usage stratégique », Revue Droit de l'Immatériel, n°77, 1er décembre 2011. Disponible sur : www.lamyline.fr [consulté le 16/02/2018]

114MARCHAND Jennifer. « L'accès et la réutilisation des données publiques dans le cadre de la loi pour une République numérique ». *In :* CHATRY Sylvain (dir.), GOBERT Thierry (dir.). *Numérique : nouveaux droits, nouveaux usages. Actes de colloque.* Editions mare&martin, 2017. p. 43

115ALGAN Yann, Maya BACACHE-BEAUVALLE, PERROT Anne. *Op. cit.* p. 9

116*Ibid.* 10

rendre inintelligible pour un humain, mais toujours intelligible pour la machine, l'objectif étant notamment d'empêcher les opérations de rétro-ingénierie, de cacher une copie illégitime d'un autre code source[117] ou d'empêcher que le code source soit copié. Dans cette situation, le fait que le code source soit accessible ne contribue absolument pas à la transparence de l'algorithme, puisqu'il est incompréhensible. D'ailleurs, selon la Free Software Foundation, un logiciel dont le code source est inintelligible ne peut être considéré comme libre car l'accès à un code source lisible est une condition nécessaire pour que l'utilisateur puisse exercer les quatre libertés accordées par la licence libre[118].

Ensuite, le code source peut être opaque en raison de sa complexité. En effet, bien qu'il soit rédigé de manière intelligible, avec une syntaxe claire, il peut être techniquement complexe et difficile à comprendre, même pour un programmeur averti. Dans ce cas, l'ouverture du code source doit nécessairement s'accompagner de commentaires et d'une documentation afin que celui-ci puisse être considéré comme contribuant à la transparence du logiciel. Aussi, l'explication de la logique de l'algorithme, qui peut être fournie par le pouvoir public, peut ici permettre de mieux comprendre le code source.

Si la fourniture d'un code source intelligible, commenté et documenté peut permettre de comprendre le fonctionnement de la plupart des logiciels, ces informations peuvent, dans certains cas, s'avérer insuffisantes pour comprendre leur fonctionnement. Il s'agit notamment du cas particulier des algorithmes d'apprentissage automatique – également appelés algorithmes d'apprentissage machine ou algorithmes de *machine learning* – que les pouvoirs publics peuvent être amenés à utiliser. Un algorithme d'apprentissage machine est un algorithme conçu dans l'objectif de résoudre un problème sans qu'il ait été explicitement programmé à le faire; il est conçu de telle

117CHILOWICZ Michel. *Recherche de similarité dans du code source.* ROUSSEL Gilles (dir. De Recherche). Thèse de doctorat. Informatique. Université Paris-Est. 2010. p.59. Disponible sur : https://pastel.archives-ouvertes.fr/tel-00587628/document [consulté le 7/08/2018]

118Free Software Foundation, « Qu'est-ce que le logiciel libre ? ». Disponible sur : https://www.gnu.org/philosophy/free-sw.fr.html [consulté le 7/08/2018]

sorte qu'il apprend à effectuer cette tâche en se basant sur un ensemble de données[119]. Ainsi, le fonctionnement d'un algorithme d'apprentissage dépend étroitement de l'ensemble de données qu'il a précédemment traité pour apprendre à résoudre des problèmes. Comme l'expliquent Danièle Bourcier et Primavera De Filippi, pour ce type d'algorithme, il est impossible de prévoir leur fonctionnement en s'appuyant uniquement sur l'analyse de leur code source ; il est nécessaire d'avoir accès à la fois au code source et à l'ensemble des données qui ont servi à l'algorithme d'apprendre à fonctionner[120]. Cela est d'autant plus nécessaire que lorsque l'algorithme apprend et évolue au fur et à mesure, il génère un certain nombre de données qui peuvent être inintelligibles, même pour un programmeur averti[121].

Ainsi, l'accès au code source, selon la complexité ou le type d'algorithme, peut contribuer plus ou moins fortement à la transparence de ce dernier. Ainsi, pour les algorithmes les plus élémentaires, l'accès au code source permet de connaître de manière exhaustive toutes ses fonctionnalités et ainsi contribue à la transparence de ces derniers de manière absolue. En revanche, pour les algorithmes plus complexes, l'accès au code source doit nécessairement s'accompagner de commentaires et d'une documentation, afin que l'algorithme puisse être considéré comme transparent. Enfin, pour certains types d'algorithmes, et ici spécifiquement pour les algorithmes d'apprentissage machine auxquels les pouvoirs publics peuvent recourir, le simple accès au code source contribue insuffisamment à la transparence de l'algorithme, puisqu'il ne permet pas à lui seul de comprendre et de prévoir son fonctionnement[122] ;

119AMINI Massih-Rezah. *Apprentissage machine : de la théorie à la pratique.* Paris : Editions Eyrolles, 2015. p. 1

120BOURCIER Danièle, DE FILIPPI Primavera. « Les algorithmes sont-ils devenus le langage ordinaire de l'administration ? ». In : KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). Lectures critiques du Code des relations entre le public et l'administration. LGDJ, 2018. p. 204

121BURREL Jenna. « How the machine ' thinks ' : Understanding opacity in machine learning algorithms ». Big Data & Society, Volume 3, Issue 1, January-June 2016. p. 10

122BOURCIER Danièle, DE FILIPPI Primavera. *Op. cit.* p. 204

dans cette situation, l'accès au code source doit s'accompagner d'un accès aux données qui ont servi à l'algorithme pour construire sa logique[123], afin de le considérer comme transparent.

Néanmoins, l'accès au code source apparaît comme une indispensable contribution à la transparence de l'algorithme du pouvoir public, puisqu'il décrit concrètement et exhaustivement les instructions du programme, contrairement à la simple explication de la logique de l'algorithme qui peut omettre volontairement ou involontairement de divulguer certaines fonctionnalités de ce dernier.

Certains pouvoirs publics recommandent la communication du code source, tandis que d'autres estiment qu'il n'est pas nécessaire de communiquer le code source pour contribuer à la transparence des algorithmes des pouvoirs publics.

Le Conseil d'État, dans son étude annuelle de 2014 sur le numérique et les droits fondamentaux a précisé que doit notamment être poursuivi l'objectif de mettre en place des garanties de procédure et de transparence afin de « donner aux individus des garanties appropriées concernant les algorithmes prédictifs utilisés pour prendre des décisions à leur égard »[124]. Ainsi, il explique que l'usager devrait avoir le droit de connaître les données utilisées par l'algorithme, d'obtenir une explication sur le raisonnement de celui-ci et de présenter ses observations[125]. Néanmoins, pour le Conseil d'État, il n'est pas nécessaire de connaître le fonctionnement interne de l'algorithme pour en déceler les caractéristiques, ces dernières pouvant être révélées en recourant à « une approche dite d'ingénierie inversée »[126] (rétro-ingénierie) qui consiste à soumettre l'algorithme à une série de tests. Le Conseil d'État conforte son argument en précisant que c'est cette approche qui a permis à une chercheur de

123 BOURCIER Danièle, DE FILIPPI Primavera. « Les algorithmes sont-ils devenus le langage ordinaire de l'administration ? ». In : KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Lectures critiques du Code des relations entre le public et l'administration. LGDJ, 2018.* p. 204

124 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n° 65. Paris : La documentation française, 2014. p. 237

125 *Ibid.* p. 239

126 *Ibid.* p. 301

l'université d'Harvard d'établir que des discriminations illicites étaient mises en œuvre dans des moteurs de recherche[127]. Certes l'ingénierie inversée peut permettre de révéler les caractéristiques et le fonctionnement d'un algorithme opaque, néanmoins la technique peut être coûteuse en temps et en argent et certaines caractéristiques peuvent restées cachées tant que les bons tests n'ont pas été effectués. Le recours à l'ingénierie inversée peut être conçue comme une solution de secours pour l'usager qui fait face à un algorithme opaque, néanmoins, elle ne peut pas être une justification à l'opacité des algorithmes des pouvoirs publics, puisqu'elle ne permet pas systématiquement d'en révéler toutes les caractéristiques.

De même, en avril 2018, la Commission européenne, tout en expliquant que la transparence des algorithmes est primordiale, en raison du fait que ces derniers sont à la base de plus en plus de décisions qui concernent la vie quotidienne, précise que la transparence algorithmique n'implique pas la divulgation du code source en tant que tel mais peut prendre diverses formes (explication utile, rapports aux autorités compétentes)[128].

La CNIL, en revanche, dans sa recommandation de 2003 relative à la sécurité des systèmes de vote électronique, a estimé que dans le cas d'une élection organisée par une collectivité publique, le code source du système de vote électronique devrait être accessible sans restriction afin que puissent être réalisées toutes les expertises jugées nécessaires[129]. La formule ne sera pas exactement reprise dans la recommandation de 2010, mais la CNIL rappelle cette exigence d'une expertise préalable du système de vote électronique qui doit notamment porter sur le code source du logiciel[130].

---

127 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n°65. Paris : La documentation française, 2014. p. 301

128 Commission européenne. « Une approche européenne en matière d'intelligence artificielle ». *Questions et réponses.* Bruxelles, le 25 avril 2018

129 CNIL. Délibération n°03-036 du 1 juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, point I 1)

130 CNIL. Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, point I 1)

Enfin, la Cour des comptes, dans son rapport public annuel de 2018, vient dire que les usagers ne peuvent pas connaître l'ensemble des fonctionnalités d'un logiciel propriétaire puisque le code source n'est pas accessible[131]. Ainsi, pour la Cour des comptes, pour connaître l'ensemble des fonctionnalités d'un logiciel, l'accès au code source est une condition indispensable.

131 Cour des comptes, *Rapport public annuel 2018*, Février 2018. p. 152

§2) Diversité des destinataires et des contributeurs à la transparence des algorithmes des pouvoirs publics

L'algorithme peut être transparent à l'égard de différentes personnes, selon que la transparence est directe ou indirecte. Aussi, plusieurs types de personnes peuvent contribuer à la transparence d'un algorithme utilisé par un pouvoir public.

A) Une diversité des possibles destinataires de la transparence : la distinction entre une transparence directe et une transparence indirecte[132]

La distinction entre transparence directe et transparence indirecte a été décrite par Chantal Enguehard, à propos de la transparence des opérations électorales[133]. Elle explique que la transparence des opérations électorales est directe lorsque l'électeur « peut constater, à l'ouverture du bureau, que l'urne est vide : il peut la voir, la toucher, constater sa vacuité par ses propres sens »[134]. En revanche, la transparence est indirecte lorsque « elle s'exerce via un intermédiaire humain ou logiciel privant l'électeur de sa capacité de contrôle car, dans ce cas, l'électeur doit accorder sa confiance à cet intermédiaire susceptible d'erreur, de tromperie ou de malveillance, sans pouvoir vérifier lui-même l'effectivité des mesures prises, ou la réalité des informations qui lui sont transmises »[135].

Cette distinction avancée par Chantal Enguehard peut se transposer à la transparence des algorithmes des pouvoirs publics. Ainsi, la transparence de ces derniers est directe si les intéressés ont les moyens de contrôler eux-mêmes leur fonctionnement en ayant accès directement aux éléments contribuant à la transparence de

132 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». *In :* FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie.* Paris : L'Harmattan, 2011. p. 86

133 *Ibid.*

134 *Ibid.*

135 *Ibid.* p.86-87

l'algorithme. Par exemple, la transparence sera considérée comme directe si le code source est communiqué à l'intéressé, ou rendu public. En revanche, la transparence sera considérée comme indirecte si ce n'est pas l'intéressé qui a accès aux éléments contribuant à la transparence de l'algorithme mais c'est par exemple un organisme public ou privé de contrôle.

En France, contrairement aux opérations de vote par bulletin papier dont la transparence est directe, les électeurs pouvant observer le déroulement du scrutin, tout au long de la journée[136], les systèmes de vote électronique sont quant à eux transparents de façon indirecte. En effet, l'article R176-3 du code électoral dispose que « préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section »[137] (secret du vote, sincérité du scrutin) et l'article R176-3-1 dispose que « Les opérations de vote par voie électronique sont placées sous le contrôle d'un bureau du vote électronique »[138]. Pour Chantal Enguehard, et dans le cas spécifique des opérations électorales, la transparence doit être directe pour être effective car dans une situation de transparence indirecte, l'électeur peut être amené à douter de la parole de l'intermédiaire et donc ne pas faire confiance au système de vote[139].

La transparence indirecte en revanche peut avoir pour intérêt de préserver le secret industriel du concepteur du logiciel, la communication ou la publicité des éléments de l'algorithme pouvant y porter atteinte[140]. Mais la transparence indirecte ne permet pas à l'intéressé de constater lui même le bon fonctionnement de l'algorithme, l'absence de

136ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». Science et pseudo-Sciences, n°320, avril 2017. Disponible sur : http://www.pseudo-sciences.org/spip.php?article2800 [consulté le 3 août 2018]

137Code électoral. Article R176-3

138Code électoral. Article R176-3-1

139ENGUEHARD Chantal. « Transparence, élection et vote électronique ». *In :* FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie.* Paris : L'Harmattan, 2011. p.86-87

140VALAT Grimaud. « Propositions pour un encadrement du régime juridique des logiciels ». *Revue Le Lamy Droit de l'Immatériel,* n°123, 1er février 2016. p. 5

fraudes et de dysfonctionnements et ne lui permet pas non plus de rassembler les preuves de violation du droit afin de les faire constater par les juridictions compétentes[141].

Aussi, confier le contrôler des algorithmes uniquement à un organisme de contrôle fait peser le risque de restreindre ce contrôle à un nombre réduit de personnes qui ne sont pas forcément suffisamment compétentes. En conséquence, si la transparence indirecte est choisie, il est nécessaire de veiller à ce que l'organisme de contrôle soit composé de personnes correctement formées. Dans son rapport public de 2014 sur le numérique et les droits fondamentaux, le Conseil d'État a ainsi avancé que pour que la CNIL dispose des moyens adéquats pour contrôler les algorithmes, il était nécessaire de renforcer ses moyens humains « par le recrutement de spécialistes dotées de compétences adéquates »[142].

Enfin, ne rendre l'algorithme transparent qu'à l'égard d'un organisme de contrôle peut faire peser le risque que des dysfonctions soient volontairement omises en raison de la présence de personnes dans l'organisme ayant intérêt à ignorer les dysfonctions. Ainsi, concernant les opérations de vote électronique belges, il était reproché que les experts désignés pour déceler les imperfections et les dérives étaient choisis par les assemblées parlementaires elles-mêmes et étaient donc d'une certaine manière juges et parties[143]. Il est important donc de s'assurer de l'indépendance des organismes de contrôle s'il est fait le choix d'une transparence indirecte.

Ensuite, plusieurs personnes peuvent contribuer à la transparence des algorithmes des pouvoirs publics.

---

141 ENGUEHARD Chantal. « Transparence, élection et vote électronique ». *In :* FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie.* Paris : L'Harmattan, 2011. p.99-100

142 *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n° 65. Paris : La documentation française, 2014. p. 301

143 DELPÉRÉE Francis. « Le vote électronique en Belgique ». *In :* FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie.* Paris : L'Harmattan, 2011. p. 22

B) Une diversité des possibles contributeurs à la transparence

Tout d'abord, le concepteur lui même peut contribuer à la transparence de l'algorithme utilisé par le pouvoir public, en publiant ou communiquant lui même les éléments de ce dernier (documentation, code source, etc). Il peut partager ces éléments avec le public, sur son site internet par exemple, ou uniquement avec le pouvoir public. En effet, les algorithmes des pouvoirs publics peuvent être opaques pour les usagers mais peuvent l'être aussi pour le pouvoir public lui même. C'est le cas lorsque le concepteur distribue son logiciel sous une licence propriétaire, ce qui peut n'impliquer à l'utilisateur la divulgation d'aucun élément contribuant à la transparence du logiciel. En revanche, si le concepteur distribue son logiciel sous une licence libre, par exemple, il est contraint de fournir à l'utilisateur le code source[144].

Ensuite le pouvoir public lui même peut contribuer à la transparence de ses algorithmes, en publiant, ou en communiquant à l'intéressé qui en fait la demande, les éléments de ce dernier. Le pouvoir public peut ainsi, par exemple, publier sur un site internet les codes sources de ses logiciels, publier une liste des logiciels qu'il utilise, la documentation, etc.

Enfin, le citoyen, l'usager, peut lui-même contribuer à la transparence de l'algorithme du pouvoir public. Tout d'abord, en communiquant à son tour les informations qu'il a obtenu du concepteur de l'algorithme ou du pouvoir public, si le droit en vigueur le permet, ou en prenant le risque de violer le droit si celui-ci ne le permet pas. En France, l'article L122-6 du code de la propriété intellectuelle dispose que la reproduction du logiciel doit être soumise à l'autorisation de l'auteur du logiciel. Ainsi reproduire le logiciel, en partageant son code source notamment, sans autorisation de l'auteur constituerait une violation de son droit d'auteur. En revanche, si les informations ont été fournies par le pouvoir public, le droit peut permettre que celles-ci

144Free Software Foundation, « Qu'est-ce que le logiciel libre ? ». Disponible sur : https://www.gnu.org/philosophy/free-sw.fr.html [consulté le 7/08/2018]

puissent être librement réutilisées par l'intéressé. Ainsi, en France, le CRPA prévoit en son article L321-1 que « Les informations publiques figurant dans des documents communiqués ou publiés par les administrations mentionnées au premier alinéa de l'article L. 300-2 peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus »[145]. Néanmoins, si le document contient des informations sur lesquelles des tiers détiennent des droits de propriété intellectuelle, celles ci ne seront pas considérées comme informations publiques et ne peuvent donc pas être réutilisées par l'intéressé, en vertu de l'article L321-2 du CRPA.

L'usager peut également contribuer à la transparence de l'algorithme en communiquant des informations qu'il a acquit de lui-même, en recourant à des techniques d'ingénierie inversée. En revanche, il faut savoir que l'usager en communiquant de telles informations peut être poursuivi et condamné pour contrefaçon. En effet, en France, l'ingénierie inversée est strictement encadrée par le droit. Ainsi, l'article L122-6-1 du code de la propriété intellectuelle prévoit un certain nombre de conditions pour que des opérations de rétro ingénieries puissent être menées sans l'autorisation du concepteur du logiciel. Tout d'abord, l'article pose comme condition première que ces opérations doivent être indispensables « pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels »[146]. Ensuite, doivent être réunies trois conditions cumulatives à savoir que « 1° ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ; 2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ; 3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité »[147]. L'article poursuit en disposant que : « les informations ainsi obtenues ne peuvent être : 1° Ni utilisées à des fins autres que la réalisation de

145CRPA. Article L321-1
146CPI. Article L122-6-1
147CPI. Article L122-6-1

l'interopérabilité du logiciel créé de façon indépendante ; 2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ; 3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur. »[148].

Ainsi, sans l'autorisation de l'auteur du logiciel, il est très difficile pour l'utilisateur de contribuer à la transparence de ce dernier sans courir le risque d'être condamné pour contrefaçon. La cour d'appel de Caen a ainsi condamné une personne qui avait décompilé le logiciel Skype puis avait partagé sur internet le code source obtenu alors que ce n'était pas nécessaire à l'interopérabilité[149].

148CPI. Article L122-6-1

149CA de Caen, chambre des appels correctionnels, 18 mars 2015. S.O. c/ Skype Ltd et Skype Software SARL.

Section 2 : Une diversité d'outils de garantie de la transparence des algorithmes des pouvoirs publics

Les pouvoirs publics peuvent recourir à divers outils de garantie de la transparence de leurs algorithmes. Ils peuvent ainsi recourir à des instruments contraignants (règlement, lois, décrets, etc) (§1) mais ils peuvent également assurer cette transparence en choisissant de recourir à des solutions libres ou *open source* (§2).

§1) Instruments normatifs de garantie de la transparence des algorithmes

La transparence des algorithmes est prévue par le droit de l'Union européenne et aussi dans le droit interne des États.

A) Union Européenne et transparence des algorithmes

Le droit de l'Union européenne prévoit des règles, dans le Règlement général sur la protection des données (RGPD), concernant les décisions prises sur le fondement d'un algorithme, ainsi que concernant la transparence de ce dernier.

Avant le RGPD, une directive 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, est venu régir ce qu'il désigne comme étant les « décisions automatisées » , c'est à dire les décisions prises sur le fondement d'un algorithme. Celle-ci consacre en son article 15 paragraphe 1 le droit à toute personne de « de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit,

sa fiabilité, son comportement, etc. »[150], sauf exceptions. Aussi, la directive prévoit en son article 12 que « les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement: […] la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'article 15 paragraphe 1 »[151]. Le préambule de la directive affirme que ce droit de connaître la logique du traitement automatisé « ne doit pas porter atteinte au secret des affaires ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel ; que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée »[152]. Ainsi la directive de 1995 impose aux États membres de garantir dans leur droit interne une transparence des algorithmes – au moins dans le cas où ils seraient le seul fondement d'une décision – mais le droit d'accès à « la connaissance de la logique » de l'algorithme prévu par la directive ne signifie pas la consécration d'un droit d'accès au code source, puisque la communication de ce dernier est susceptible de porter atteinte au secret des affaires ou au droit d'auteur.

Cette directive n'est plus en vigueur depuis le 25 mai 2018 car elle a été abrogée et remplacée par le RGPD.

La décision prise sur le fondement d'un algorithme est régie par l'article 22 du Règlement général sur la protection des données (RGPD), qui y fait référence sous l'expression de « Décision individuelle automatisée, y compris le profilage ». L'article 22 dispose qu'une personne a le droit de ne pas faire l'objet d'une décision exclusivement fondée sur un traitement automatisé, sauf exceptions. Dans le cas où une telle décision serait prise, les articles 13, 14 et 15 du RGPD disposent que, la personne concernée a le droit notamment d'être informée par le responsable du traitement de « l'existence d'une prise de décision automatisée [...] et, au moins en

150 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, Article 15

151 *Ibid.* Article 12

152 *Ibid.* (41)

pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée »[153].

En conséquence, le droit de l'Union européenne prévoit qu'une personne a le droit d'être informée qu'une décision administrative prise à son égard a été prise sur le seul fondement d'un algorithme qui traite des données à caractères personnelles le concernant et a le droit d'obtenir des informations sur la logique de cet algorithme. Ainsi, une transparence minimale des algorithmes est consacrée dans le RGPD, mais ce dernier n'est pas assez précis sur la forme des informations auxquelles aura accès l'intéressé. La Commission européenne a affirmé que la transparence algorithmique sera abordée dans des lignes directrices en matière d'éthique pour l'Intelligence artificielle, qui seront élaborées à la fin de l'année 2018[154]. Ainsi, il faudra attendre la publication de ces lignes directrices pour en savoir d'avantage sur les informations auxquelles le RGPD permet à l'usager d'accéder, lorsqu'il a fait l'objet d'une décision prise sur le seul fondement d'un traitement automatisé. Néanmoins, la Commission européenne a déjà prévenu que la transparence algorithmique ne signifie pas la divulgation du code source, mais que celle-ci peut prendre différentes formes, selon la situation (explication utile, rapports aux autorités compétentes)[155].

Ici il est fait référence aux décisions algorithmiques administratives, mais la directive et le RGPD ont un champ d'application plus large (entreprises publiques, entreprises privées, etc).

Les États garantissent la transparence dans leur droit interne. Ici, quelques exemples, dont la France, sont avancés.

153 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), articles 13, 14 et 15

154 Commission européenne. « Une approche européenne en matière d'intelligence artificielle ». *Questions et réponses.* Bruxelles, le 25 avril 2018.

155 *Ibid.*

B) Transparence des algorithmes des pouvoirs publics dans le droit interne

En France, la loi de 1978 dite Informatique et libertés est le premier texte venu encadrer les algorithmes utilisés comme fondement d'une décision. Ainsi, l'article 2 de la loi, telle que rédigée en 1978, disposait que « aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatisé d'informations, donnant une définition du profil ou de la personnalité de l'intéressé. Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé »[156]. L'article 3 quant à lui disposait que « toute personne a le droit de connaître et de contester les informations et les raisonnement utilisés dans les traitements automatisés dont les résultats lui sont opposés »[157]. Ainsi, une première forme d'exigence de transparence de l'algorithme, et à la demande de l'intéressé, est posée dans la loi de 1978. Néanmoins, aucune précision n'était apportée sur le type d'informations auquel l'intéressé pourra accéder. Des précisions seront apportées par la loi de 1978, dans sa rédaction issue de la loi du 6 août 2004. Avec la loi de 2004, les dispositions de l'article 2 et 3 sont reformulées et dorénavant prévues aux articles 10 et 39. Ainsi, l'article 39 dispose que « - I. - Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir : [...] « 5° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé »[158]. Jusqu'ici, la formulation de l'ancien article 2 de la loi de 1978 est reprise par l'article 39, dans sa rédaction issue de la loi de 2004. Seulement, une précision est

156 Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF du 7 janvier 1978. p. 227. Article 2

157 *Ibid.* Article 3

158 Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF n°182 du 7 août 2004. p. 14063. Article 39

ajoutée par cette dernière puisque l'article poursuit en disposant que « toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle. »[159].

La loi de 1978 a été modifiée à de nombreuses reprises, sa dernière rédaction étant issue de la loi du 20 juin 2018 relative à la protection des données personnelles. La Loi de 2018 a modifié la loi de 1978 afin de l'adapter au RGPD. Ainsi, l'article 10 est modifié afin d'inclure les exceptions prévues par l'article 22 du RGPD, c'est à dire les exceptions où il est finalement possible qu'une une décision soit prise sur le seul fondement d'un traitement automatisé.

En plus de la loi de 1978, le code des relations entre le public et l'administration (CRPA), prévoit un certain nombre d'articles concernant spécifiquement les algorithmes utilisés par l'administration comme fondement à une décision administrative. Ainsi l'article 4 de la loi pour une République numérique a créé dans le CRPA un article L311-3-1 qui dispose que « sous réserve de l'application du 2° de l'article L. 311-5,une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande. »[160]. Ainsi, pèse sur l'administration l'obligation d'informer l'intéressé que la décision a été prise sur le fondement d'un algorithme et une obligation de transparence de ce dernier, si l'intéressé en fait la demande. L'article R311-3-1-2 précise les informations auxquelles l'intéressé, qui en fait la demande, se verra communiqué : « 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2° Les données traitées et leurs sources ; 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; 4° Les

159Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF n°182 du 7 août 2004. p. 14063. Article 39

160CRPA Article L311-3-1

opérations effectuées par le traitement »[161]. On constate que l'article n'est pas très clair concernant la communication du code source. Néanmoins, la transparence de ce dernier découle de l'article L300-2 du CRPA qui reconnaît les codes sources des logiciels de l'administration comme documents administratifs. Les administrations sont donc tenues de publier en ligne ou de communiquer ces derniers aux personnes qui en font la demande, en vertu de l'article L311-1 du CRPA – sauf dans les cas prévus par les article L311-5 et L311-6 du CRPA. Aussi, l'article L312-1-3 du CRPA dispose que les administrations, « sous réserve des secrets protégés en application du 2° de l'article L. 311-5, […] publient en ligne les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions lorsqu'ils fondent des décisions individuelles »[162]. Ainsi, de la lecture combinée de tous ces articles, il découle une obligation de transparence des algorithmes des administrations, qu'ils fondent une décision individuelle ou non (l'article L300-2 mentionne les codes sources sans distinction), et cette transparence implique un accès au code source. Enfin, l'article L321-1 du CRPA disposent que « les informations publiques figurant dans des documents communiqués ou publiés par les administrations […] peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus »[163]. Les informations concernant le traitement algorithmique à l'origine de la décision, y compris le code source, peuvent donc être réutilisés par l'intéressé. Des limites sont toutefois posées par le CRPA. Ainsi, l'article l321-2 du CRPA précise notamment que « ne sont pas considérées comme des informations publiques, pour l'application du présent titre [Titre II : La réutilisation des informations publiques], les informations contenues dans des documents […] sur lesquels des tiers détiennent des droits de propriété intellectuelle »[164]. Ainsi, les informations concernant le traitement algorithmique à l'origine de la décision peuvent être réutilisées par l'intéressé à condition que des tiers

161CRPA, Article R311-3-1-2
162CRPA. Article L312-1-3
163CRPA, Article L321-1
164CRPA. Article L321-2

ne détiennent pas des droits de propriété intellectuelle dessus. Ainsi, si l'administration a eu recours à un algorithme distribué sous licence propriétaire, l'usager ne sera pas libre de réutiliser les informations concernant l'algorithme.

La reconnaissance du code source comme document administratif est la consécration par la Loi pour une République numérique de la jurisprudence de la Commission d'accès aux documents administratifs (CADA). En effet, la CADA, dans son avis n° 20144578 du 8 janvier 2015, relatif au code source du logiciel simulant le calcul de l'impôt sur les revenus des personnes physiques développé par la direction générale des finances publiques (DGFIP), et dans son avis 20161989 du 23 juin 2016, relatif au code source de la plate-forme Admission post bac (A.P.B), a estimé que les fichiers informatiques constituant le code source revêtaient le caractère de documents administratifs, au sens de l'article L300-2 du CRPA, et étaient communicables à toute personne, conformément à l'article L311-1 du CRPA et réutilisables par toute personne qui le souhaite à d'autres fins que celles de la mission de service public de l'administration concernée, en vertu de l'article L321-1 du CRPA. La jurisprudence de la CADA a été confirmée par le Tribunal administratif de Paris dans un jugement n°1508951/5-2 du 10 mars 2016.

En Bulgarie, les algorithmes développés spécifiquement pour l'administration sont transparents, sans qu'il soit nécessaire que l'intéressé en fasse la demande préalable. En effet, la loi pour la Gouvernance électronique a été modifiée en 2016 pour prévoir que les logiciels développés spécifiquement pour le gouvernement doivent être *open source* et développés dans un répertoire public[165]. Le conseiller du vice-premier ministre Bozhidar Bozhanov explique qu'avec l'ouverture des codes sources, naît l'espoir d'une meilleure sécurité des algorithmes du gouvernement, l'opacité ayant été, avant, la raison pour laquelle de nombreuses failles de sécurité dans les sites internet gouvernementaux n'ont pas été corrigées pendant des années. Aussi, il explique que, finalement, il est normal pour les logiciels du gouvernement d'être transparents pour le

165ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ (Loi sur la Gouvernance électronique) (dernière modification le 9 décembre 2016), article 58a

contribuable, puisque c'est l'impôt qui les finance. Il précise enfin que cela n'implique pas que les logiciels développés par Microsoft et utilisés par le gouvernement, par exemple, seront obligatoirement open source, mais que les futurs logiciels produits sur mesure pour le gouvernement seront visibles et accessibles à tous ; les solutions qui ont été acquis antérieurement ne sont en revanche pas affectés par la réforme[166].

Aussi, en Italie, le paragraphe 1 de l'article 69 du Code de l'administration digitale dispose que les administrations publiques ont l'obligation de mettre à disposition, dans un répertoire public sous licence ouverte, le code source complet, et documenté, des programmes informatiques qu'elles utilisent et qui ont été réalisés sur ses indications spécifiques[167].

En France, on constate que le droit n'a toujours pas consacré d'obligation d'ouverture et de publication systématique des codes sources, comme c'est le cas en Italie et en Bulgarie pour les algorithmes développés pour l'administration. Il est certes consacrée une certaine transparence des algorithmes des pouvoirs publics, mais elle est souvent conditionnée au fait que l'usager doit en faire préalablement la demande. Néanmoins, sans passer nécessairement par des instruments contraignants, les pouvoirs publics ont mené ponctuellement des politiques d'ouverture et de transparence de leurs algorithmes.

Ainsi, la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) a lancé une stratégie, « l'État plateforme », dont le coup d'envoi était un Hackathon organisé les 18 et 19 juin 2015[168]. L'objectif de cette

166BOZHANOV Bozhidar. « Bulgaria Got a Law Requiring Open Source ». *Thepolicy.us*, 4 Juillet 2016. Disponible sur : https://thepolicy.us/bulgaria-got-a-law-requiring-open-source-98bf626cf70a [consulté le 20/08/2018]

167DECRETO LEGISLATIVO 7 marzo 2005, n. 82 (modifié par le Decreto Legislativo 13 dicembre 2017, n. 217) , Codice dell'amministrazione digitale. (GU n.112 del 16-5-2005 - Suppl. Ordinario n. 93), article 69

168MARZIN Jacques. « L'État plateforme donnera naissance à de nouveaux services publics numériques ». 17 septembre 2015. Disponible sur : http://www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/etat-plateforme-tribune-marzin [consulté le 20 août 2018]

stratégie est de faciliter la circulation des données entre les organismes publics afin de fournir un service plus simple, fluide et transparent pour l'usager[169]. Cette stratégie, qui s'étend à l'ensemble de la sphère publique, repose notamment sur l'ouverture et le partage des API (accronyme d'*Application Programming Interface.* Les API sont des interfaces de programmation d'applications destinées aux programmeurs[170] et qui permettent la communication et l'échange de données entre applications[171]), des données et des codes sources, comme l'explique la Cour des comptes dans son rapport public annuel de 2018[172]. C'est dans le cadre de cette stratégie qu'Etalab organise un Hackathon en avril 2016 , en coordination avec la DGFIP, autour de l'ouverture du code source du calculateur de l'impôt[173].

Aussi, la France a rejoint en avril 2014 le Partenariat pour un gouvernement ouvert (PGO). Lancé le 20 septembre 2011, le PGO a pour objectif de rendre les gouvernements plus transparents, plus responsables et plus réactifs envers leurs propres citoyens, avec l'objectif ultime d'améliorer la gouvernance et la qualité des services que les citoyens reçoivent[174]. Les pays qui rejoignent le PGO s'engagent ainsi à respecter la Déclaration du gouvernement ouvert dont les grands principes sont : la transparence de l'action publique, la participation des citoyens à l'élaboration et à l'évaluation des politiques publiques, l'intégrité de l'action publique et des agents publics, l'utilisation des nouvelles technologies en faveur de l'ouverture et de la recevabilité[175]. Ils doivent élaborer tous les deux ans des plans d'action nationaux qui

169MARZIN Jacques. « L'État plateforme donnera naissance à de nouveaux services publics numériques ». 17 septembre 2015. Disponible sur : http://www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/etat-plateforme-tribune-marzin [consulté le 20 août 2018]

170LILEN Henri. *Dictionnaire informatique et numérique.* Paris : Editions First-Gründ, 2011. Api

171Cour des comptes, *Rapport public annuel 2018*, Février 2018. p. 149

172Cour des comptes, *Rapport public annuel 2018*, Février 2018. p. 149

173ALGAN Yann, Maya BACACHE-BEAUVALLE, PERROT Anne. *Op. cit.* p. 10

174Open Government Partnership. « Mission and Strategy ». Disponible sur : https://www.opengovpartnership.org/mission-and-strategy [consulté le 14/08/2018]

175Le blog d'Etalab. « Le Partenariat pour un gouvernement ouvert (« PGO », ou Open Government Partnership – « OGP ») ». Disponible sur : https://www.etalab.gouv.fr/ogp [consulté le 14/08/2018]

rassemblent leurs engagements. Ainsi, dans le plan d'action national 2018-2020, la France s'est engagée à améliorer la transparence des algorithmes des pouvoirs publics ainsi que leurs codes sources[176].

Sans recourir à des instruments contraignants, les pouvoirs publics peuvent également garantir la transparence de leurs algorithmes en faisant le choix de recourir à des logiciels distribués sous des licences libres ou *open source*.

176 Plan d'action national 2018-2020 de la France dans le cadre du Partenariat pour un gouvernement ouvert, engagement 6

§2) Transparence pouvant être garantie par l'utilisation de logiciels sous licences ouvertes

La transparence des algorithmes des pouvoirs publics peut également être assurée par le recours à des logiciels *open source* ou libres, c'est à dire des logiciels distribués sous des licences qui accordent un certain nombre de droits à leurs bénéficiaires. En plus de la transparence, le recours à ce type de logiciels peut présenter un certain nombre d'intérêts qui peuvent pousser le pouvoir public à favoriser, et promouvoir, le recours à ces derniers au détriment des logiciels propriétaires

A) Intérêts de recourir à des logiciels sous licences ouvertes

Il est entendu par « licences ouvertes » les licences dites libres et *open source*. D'après la Free Software Foundation, un logiciel est libre lorsqu'il est distribué sous une licence qui assure à l'utilisateur quatre libertés essentielles, à savoir la liberté d'exécuter le logiciel librement et pour n'importe quel usage, la liberté d'étudier et de modifier le logiciel, la liberté de redistribuer des copies et la liberté de distribuer des copies modifiées du logiciel. Pour que soient effectivement exercées ces libertés, la Free Software Foundation précise que l'accès au code source est une condition nécessaire[177]. Même si « pratiquement tous les logiciels libres sont open source et presque tous les logiciels open source sont libres »[178], il existe des différences entre ces deux catégories de logiciels, comme l'explique la Free Software Foundation. Selon l'Open source Initiative, un logiciel est open source si il est distribué sous une licence qui respecte les dix critères énoncés par l'organisation[179]. Notamment, pour que le logiciel puisse être considéré comme open source, il doit inclure un code source non

177Free Software Foundation, « Qu'est-ce que le logiciel libre ? ». Disponible sur : https://www.gnu.org/philosophy/free-sw.fr.html [consulté le 7/08/2018]

178Free Software Foundation. « Catégories de logiciels libres et non libres ». Disponible sur https://www.gnu.org/philosophy/categories.html [consulté le 11/08/2018]

179Open Source Initiative. « The Open Source Définition ». Disponible sur : https://opensource.org/osd [consulté le 11/08/2018]

offusqué, ou l'acquisition de ce dernier doit être possible moyennant un coût qui n'excède pas un coût raisonnable de reproduction et qui puisse de préférence être téléchargé sur internet. Aussi, la distribution du code source modifié ne doit pas être restreinte par la licence, sauf si cette dernière permet la distribution de fichiers patch avec le code source[180].

Ces types de licences, par les droits qu'elles accordent à leurs bénéficiaires, s'opposent aux licences dîtes propriétaires, qui bien que parfois peuvent permettre un accès au code source, ne garantissent pas les libertés accordées par les licences ouvertes.

Si les licences open source apparaissent légèrement plus restrictives que les licences libres, les logiciels distribués sous ces licences ont pour point commun leur transparence, puisque leur code source est accessible. Ainsi, avec ce type de licence, l'utilisateur d'un logiciel libre ou *open source* peut étudier, modifier et même redistribuer des versions modifiées du code source. En revanche, cette obligation de divulgation du code source ne s'applique qu'à celui qui distribue le logiciel et non à celui qui utilise le logiciel libre, car l'aspect crucial du logiciel libre est qu'il laisse à l'utilisateur la liberté de coopérer ou non[181]. Ainsi, si le pouvoir public utilise un logiciel libre ou *open source*, rien ne l'oblige à publier à son tour les codes sources de ce dernier, même s'ils ont été modifiés, tant qu'il ne distribue pas le logiciel. Ainsi, la transparence de ces logiciels peut ne profiter qu'au pouvoir public. Pour que le logiciel devienne transparent à l'égard de l'usager, le pouvoir public peut soit de sa propre initiative, et à sa discrétion, publier les codes sources des logiciels libres ou open source qu'il utilise, soit recourir à des logiciels dont le code source a été publié par le distributeur et informer les usagers d'un tel recours, afin que ces derniers puissent se

180 Open Source Initiative. « The Open Source Définition ». Disponible sur : https://opensource.org/osd [consulté le 11/08/2018]

181 Foire aux questions sur les licences GNU. Disponible sur : https://www.gnu.org/licenses/gpl-faq.fr.html#GPLRequireSourcePostedPublic [consulté le 20/08/2018]

procurer eux-mêmes les codes sources – et toute autre forme d'informations susceptibles de contribuer à la transparence du logiciel – auprès du distributeur (sur son site internet, par exemple).

Pour le pouvoir public, recourir à des logiciels distribués sous des licences ouvertes peut présenter plusieurs intérêts. Ludovic SCHURR en retient quatre principaux : le recours à ces licences permet de réduire les coûts, d'augmenter l'indépendance technique, d'assurer une transparence technique et de changer plus aisément de titulaire sur les marchés[182]. En effet, la possibilité d'étudier et de modifier le code source de ces logiciels permet au pouvoir public d'avoir une certaine indépendance technique et financière car il est libre de consulter et de modifier le code source du logiciel et ainsi peut maintenir et adapter ce dernier à ses besoin, soit lui même, soit en faisant appel à un autre prestataire[183]. La transparence technique résulte du libre accès au code source permis par la licence. Au contraire, si il décide de recourir à une solution propriétaire, le pouvoir public se trouve dans une situation de codépendance avec le fournisseur[184], puisque ce dernierl est le seul à connaître l'ensemble des fonctionnalités du logiciel et est le seul à être en mesure de maintenir le logiciel.

L'autre argument en faveur d'un recours par les pouvoirs publics de logiciels sous licence ouverte, et avancé par la Cour des comptes dans son rapport public annuel de 2018, est celui de la sécurité. En effet, la Cour des comptes explique qu'en raison de cette transparence technique, l'utilisateur est en mesure de s'assurer du bon fonctionnement du logiciel, de se protéger contre les fonctions indésirables et éventuellement de modifier le logiciel afin de l'adapter à l'usage qu'il souhaite en faire. Aussi, pour la Cour, le caractère libre d'un logiciel n'est pas contraire à la sécurité de ce dernier puisqu'il y a un plus grand nombre d'utilisateurs susceptibles d'identifier et

182SCHURR Ludovic. « Logiciel libre : un panorama des évolutions jurisprudentielles et politiques publiques ». Revue Le Lamy Droit de l'immatériel, Nº 102, 1er mars 2014. p. 6-7

183FOUTEL Nathalie. « Licences libres en secteur industriel sensible : un usage stratégique », *Revue Droit de l'Immatériel,* n°77, 1er décembre 2011. p. 3-4

184*Ibid.* p. 4

de corriger les éventuelles erreurs. La Cour des comptes explique qu'en revanche, avec une solution propriétaire, il est impossible de connaître les fonctionnalités du logiciel puisque le code source est maintenu secret par l'éditeur[185].

Ainsi, recourir à des solutions libres ou open source présente de nombreux intérêts, ce qui pousse de nombreux pouvoirs publics à abandonner progressivement le recours à des solutions propriétaires pour privilégier, et promouvoir, le recours à des logiciels distribués sous licences ouvertes.

B) Les pouvoirs publics ayant fait la promotion du recours à des logiciels sous licences ouvertes

Depuis quelques années, les pouvoirs publics français mènent une politique de promotion des logiciels libres. Ainsi, le 19 septembre 2012, le Premier Ministre Jean-Marc Ayrault publie une circulaire en faveur de l'usage des logiciels libres dans l'administration et dans laquelle il constate les avantages que peut apporter l'utilisation de ces derniers à savoir notamment leur coût moindre, leur adaptabilité et leur transparence. Dans cette circulaire, il est fait référence à « un cadre de convergence des souches à privilégier dans le développement des systèmes d'information de l'État, défini en 2012 [et qui est] maintenu en concertation ministérielle »[186], qui est sensée définir « des versions de référence à privilégier [et indiquer] les solutions à abandonner »[187]. Dans ce cadre, est adopté tous les ans, depuis 2013, le socle interministériel de logiciels libres (SILL) qui présente l'ensemble des logiciels libres

185Cour des comptes, *Rapport public annuel 2018*, Février 2018

186Premier ministre, Circulaire du 19 septembre 2012, « Orientations pour l'usage des logiciels libres dans l'administration ». p. 10

187Premier ministre, Circulaire du 19 septembre 2012, « Orientations pour l'usage des logiciels libres dans l'administration ». p. 10

préconisés. Le SILL est géré par les correspondants ministériels et placé sous le contrôle de la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC)[188].

La promotion du logiciel libre a également été concrétisée dans la loi française. Ainsi, l'article 16 de la loi du 8 juillet 2013 pour la refondation de l'école de la République, qui vient modifier l'article L. 131-2 du code de l'éducation dispose que « Dans le cadre [du service public du numérique éducatif], la détermination du choix des ressources utilisées tient compte de l'offre de logiciels libres et de documents au format ouvert, si elle existe »[189]. Aussi, l'article 9 de la loi du 22 Juillet 2013 relative à l'enseignement supérieur et à la recherche, qui vient modifier l'article Article L123-4-1 du code de l'éducation, dispose que les logiciels libres doivent être utilisés en priorité[190]. Enfin, la loi du 7 octobre 2016 pour une République numérique dispose en son article 16 que « les administrations mentionnées au premier alinéa de l'article L. 300-2 du code des relations entre le public et l'administration […] encouragent l'utilisation des logiciels libres et des formats ouverts lors du développement, de l'achat ou de l'utilisation, de tout ou partie, de ces systèmes d'information »[191].

La Commission européenne mène également une stratégie pour l'usage de logiciels *open source*. En effet, en Décembre 2000, la Commission européenne a défini une stratégie concernant l'usage de logiciels open source en interne[192]. Et, cette stratégie, qui depuis a été révisée trois fois, a abouti à une augmentation de l'usage de logiciels open source sur les ordinateurs utilisés à la Commission[193]. La période 2007-2010 a été marquée par l'adoption de la European Union Public License (EUPL), qui est la

188 http://references.modernisation.gouv.fr/socle-logiciels-libres [consulté le 14/08/2018]

189 LOI n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République, article 16

190 LOI n° 2013-660 du 22 juillet 2013 relative à l'enseignement supérieur et à la recherche, article 9

191 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), Version consolidée au 19 août 2018. Article 16

192 Commission européenne. « Open Source Strategy : History ». Disponible sur : https://ec.europa.eu/info/open-source-strategy-history_en [consulté le 15/08/2018]

193 Commission européenne. « Open source software strategy ». Disponible sur : https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en#opensourcesoftwarestrategy [consulté le 15/08/2018]

première licence open source européenne et qui est à la fois utilisée par les administrations publiques, le but étant principalement d'encourager ces derniers à distribuer leurs logiciels sous licence open source, et par le secteur privé[194]. Durant cette période furent également créées un certain nombre de plate-formes communautaires supportant le développement de logiciels open source, comme l'Open Source Observatory and Repository for European public administrations (OSOR.eu) qui encourage le développement de logiciels open source destinés à être utilisé dans les administrations publiques européennes[195]. La dernière révision de la stratégie concerne la période 2014-2017 et met l'accent sur l'acquisition, la contribution à des projets de logiciels *open source* et sur le fait de présenter les logiciels développés au sein de la Commission comme étant *open source*[196]. Les objectifs pour la période 2014-2017 sont : un égal traitement entre logiciels *open source* et logiciel propriétaire lors de l'acquisition de logiciels, la participation aux communautés de logiciels *open source*, la clarification des aspects légaux relatifs à l'*open source*, des logiciels de la Commission développés de tels sorte à être *open source* et interopérables, de la transparence et une meilleure communication[197].

Enfin, un certain nombre de pouvoirs publics de pays européens ont mené une politique de promotion de l'usage de logiciels libres et *open source*. Ainsi, en 2004, l'Allemagne, dans l'objectif de mettre fin à sa dépendance technique vis à vis des logiciels propriétaires qui sont souvent américains, décide de procéder à la migration des systèmes de ses administrations vers des solutions libres[198].

194 Commission européenne. « Open Source Strategy : History ». Disponible sur : https://ec.europa.eu/info/open-source-strategy-history_en [consulté le 15/08/2018] et Commission européenne. « European Union Public License ». Disponible sur : https://ec.europa.eu/info/node/2820 [consulté le 15/08/2018]

195 *Ibid.*

196 Commission européenne. « Open source software strategy ». Disponible sur : https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en#opensourcesoftwarestrategy [consulté le 15/08/2018]

197 *Ibid.*

198 SCHURR Ludovic. « Logiciel libre : un panorama des évolutions jurisprudentielles et politiques publiques ». Revue Le Lamy Droit de l'immatériel, Nº 102, 1er mars 2014. p. 7

Aussi, d'après le site internet de la campagne « Public Money ? Public Code ! »[199], la Samtgemeinde Elbmarsch est la deuxième administration à soutenir, en signant la lettre ouverte, la campagne lancée par la Free Software Foundation Europe et qui vise à faire du Logiciel libre le standard pour les logiciels financés par l'argent public, la logique étant qu'à partir du moment où l'argent qui finance le code est public, c'est à dire que le logiciel est financé par le contribuable, le code doit à son tour être public[200] ; la première administration publique à avoir signé cette lettre ouverte ayant été la mairie de la ville de Barcelone[201]. Cette dernière a également annoncé en 2017 que, pendant le reste de son mandat, 70 % de son investissement municipal dédié au développement de nouveaux logiciels sera consacré au développement de logiciels en open source[202].

Enfin, en Italie, l'obligation de recourir à des logiciels libres est consacré dans la loi. En effet, le paragraphe 1-ter de l'article 68 du Code de l'administration digitale dispose que les administrations publiques ne peuvent être autorisées à acquérir des logiciels propriétaires que si il est impossible d'accéder à des solutions déjà disponibles au sein de l'administration publique ou à des logiciels libres ou open source[203].

199 https://publiccode.eu/ [consulté le 16/08/2018]

200 Free Software Foundation Europe. « Public Money ? Public Code ! ». Disponible sur : https://fsfe.org/campaigns/publiccode/publiccode.fr.html [consulté le 16/08/2018]

201 Free Software Foundation Europe. « "Public Money? Public Code!": plus de traductions, plus de soutiens, plus de sensibilisation ». 26 Juillet 2018. Disponible sur : https://fsfe.org/news/2018/news-20180725-01.fr.html [consulté le 16/08/2018]

202 Info Barcelona. « Barcelona's Digital Government: Open, Agile and Participatory ». 20 octobre 2017 Disponible sur : https://www.barcelona.cat/infobarcelona/en/barcelonas-digital-government-open-agile-and-particpatory_565416.html [consulté le 16/08/2018]

203 DECRETO LEGISLATIVO 7 marzo 2005, n. 82 (modifié par le Decreto Legislativo 13 dicembre 2017, n. 217), Codice dell'amministrazione digitale. (GU n.112 del 16-5-2005 - Suppl. Ordinario n. 93), article 68

Conclusion

En conclusion, on constate qu'il est aujourd'hui généralement admis que la transparence des algorithmes des pouvoirs publics est nécessaire. Ainsi, les usagers ont au moins le droit de se voir expliquer la logique des algorithmes sur le fondement desquels sont prises des décisions qui les concernent. Aussi, de plus en plus d'États consacrent dans leur droit interne la transparence des codes sources des logiciels de l'administration. Néanmoins, pour l'instant il ne s'agit souvent que d'une communication, ou d'une publication, des codes sources des logiciels conçus spécifiquement pour les pouvoirs publics et il n'est pour l'instant pas question d'une publication des codes sources des logiciels propriétaires auxquels les pouvoirs publics ont recours. Prévaut ainsi, sur ce point, toujours la protection des secrets industriels des concepteurs de logiciels sur les intérêts des individus.

Toutefois, on constate que les pouvoirs publics recourent de moins en moins à des solutions propriétaires. En effet, ils privilégient de plus en plus le recours à des logiciels distribués sous des licences *open source* ou libres. La transparence des logiciels libres et open source n'est certes pas systématique pour le public – les utilisateurs de licences ouvertes n'étant pas contraints de communiquer les codes sources s'ils ne font qu'utiliser le logiciels en interne – mais cela reste une avancée par rapport au recours à des logiciels propriétaires. En effet, ces derniers pouvaient être totalement opaques, non seulement pour le public mais également pour le pouvoir public qui y recourt.

Néanmoins, même si aujourd'hui la tendance est à une plus grande transparence des algorithmes des pouvoirs publics, une autre forme d'opacité, décrite par Jenna Burrel, persiste. Cette opacité découle du fait qu'encore aujourd'hui, la programmation, la conception d'algorithmes, la compréhension des codes sources restent des compétences spécialisées, qui ne sont maîtrisées que par une minorité de la

population[204]. En effet, comme le soulève la CNIL, « la publication pure et simple d'un code source [laisse] l'immense majorité du public, non spécialisé, dans l'incompréhension de la logique à l'œuvre »[205].

Finalement, une transparence des algorithmes n'a que peu d'intérêt si le public ne comprend pas les éléments auxquels on lui donne accès ; les algorithmes ne peuvent pas être considérés comme transparents si les éléments communiqués afin d'y contribuer sont incompréhensibles pour la majorité. C'est pourquoi, pour faire face à cette forme d'opacité, Jenna Burrel préconise la formation du public, à tous les niveaux d'éducation, à la programmation, afin qu'ils puissent être directement en position d'évaluer et de critiquer les algorithmes[206].

Sans qu'il y ait nécessairement de rapport avec la transparence des algorithmes, l'apprentissage de la programmation a été abordée par certains pouvoirs publics. Ainsi, l'ancien président des États-Unis Barack Obama, dans un discours publié en 2013 sur la chaîne Youtube Code.org, a invité tous les américains à apprendre la programmation[207] et a lui-même participé à une session de *Hour of Code,* session de programmation organisée par l'association Code.org, afin de sensibiliser le public à l'exercice cette pratique[208].

Aussi, en France, le Conseil National du Numérique, dans son rapport de 2014 « Bâtir une école créative et juste dans un monde numérique », recommande l'enseignement de l'informatique dans chaque cycle. Le CNNum recommande ainsi que soit introduit

---

204 BURREL Jenna. « How the machine ' thinks ' : Understanding opacity in machine learning algorithms ». Big Data & Society, Volume 3, Issue 1, January-June 2016. p. 4

205 Commission nationale de l'informatique et des libertés. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle.Synthèse du débat public anumé pa la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique,* Décembre 2017. p. 51

206 BURREL Jenna. *Op. cit.* p. 4

207 « Preisdent Obama asks America to learn computer science ». https://www.youtube.com/watch?v=6XvmhE1J9PY [consulté le 26/08/2018]

208 « President Obama meets with students at an Hour of Code Event ». https://www.youtube.com/watch?v=EJEBGf_uS_M

l'apprentissage de la programmation en collège sur le temps alloué à la technologie[209]. Aussi, l'ancien président François Hollande a lancé en 2014, avec la ministre de l'Éducation nationale, le « Plan numérique à l'école » qui avait pour but d'améliorer l'accès aux outils numériques en équipant les écoles de tablettes et d'ordinateur mais aussi en modifiant les programmes scolaires afin d'intégrer l'enseignement de la programmation[210]. Ainsi, depuis 2016, l'Éducation nationale a inscrit dans les programmes du collège et de l'école primaire l'apprentissage et la sensibilisation à la programmation[211].

L'apprentissage de la programmation est encouragée car elle permet la maîtrise de l'outil numérique[212] et le développement d'un esprit critique sur les technologies[213], mais indirectement elle devient aussi la dernière forme de contribution à la transparence des algorithmes des pouvoirs publics, puisqu'elle permettra dorénavant au public de comprendre les codes sources auxquels il aura accès.

209 Conseil National du Numérique. *Rapport Jules Ferry 3.0. Bâtir une école créative et juste dans un monde numérique.* Octobre 2014. p. 106

210 Déclaration de M. François Hollande, Président de la République, sur le numérique à l'école, à Paris le 16 décembre 2016. Disponible sur : http://discours.vie-publique.fr/notices/167003770.html [consulté le 26/08/2018]

211 « En 2016, le code informatique arrive à l'école ». *LeMonde.fr*, 2/11/2016. Disponible sur : https://www.lemonde.fr/sciences/article/2016/11/02/en-2016-le-code-informatique-arrive-a-l-ecole_5024344_1650684.html [consulté le 26/08/2018]

212 Déclaration de M. François Hollande, Président de la République, sur le numérique à l'école, à Paris le 16 décembre 2016. Disponible sur : http://discours.vie-publique.fr/notices/167003770.html [consulté le 26/08/2018]

213 « En 2016, le code informatique arrive à l'école ». *LeMonde.fr*, 2/11/2016.

Bibliographie

I) Documentation officielle

A) Actes contraignants

1) France

Constitution, actes législatifs et réglementaires

- Constitution du 4 octobre 1958, version consolidée au 19 août 2018

LOIS

- Loi n°69-419 du 10 mai 1969 modifiant certaines dispositions du code électoral, JORF du 11 mai 1969. p. 4723

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF du 7 janvier 1978. p. 227

- Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal, JORF du 18 juillet 1978, p. 2851

- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. JORF n°182 du 7 août 2004. p. 14063.

- Loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République. JORF n°0157 du 9 juillet 2013. p. 11379. Texte n° 1

- Loi n° 2013-660 du 22 juillet 2013 relative à l'enseignement supérieur et à la recherche, Version consolidée au 27 août 2018

- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1), Version consolidée au 19 août 2018

- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (1). JORF n°0141 du 21 juin 2018. Texte n°1

ORDONNANCES

- Ordonnance n° 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, JORF n°131 du 7 juin 2005. p. 10022. Texte n°13

- Ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France

- Ordonnance n° 2015-1341 du 23 octobre 2015 relative aux dispositions législatives du code des relations entre le public et l'administration, JORF n°0248 du 25 octobre 2015, p. 19872. Texte n° 2

DECRET

- Décret n° 2015-1342 du 23 octobre 2015 relatif aux dispositions réglementaires du code des relations entre le public et l'administration (Décrets en Conseil d'Etat et en conseil des ministres, décrets en Conseil d'Etat et décrets), JORF n°0248 du 25 octobre 2015, p. 19895. Texte n° 3

CODES

- Code électoral, version consolidée au 15 juillet 2018

- Code de la propriété intellectuelle, Version consolidée au 1 août 2018

- Code des relations entre le public et l'administration, Version consolidée au 12 août 2018.

Jurisprudence

- CA de Caen, chambre des appels correctionnels, 18 mars 2015. S.O. c/ Skype Ltd et Skype Software SARL. Disponible sur : https://www.legalis.net/jurisprudences/cour-dappel-de-caen-chambre-des-appels-correctionnels-arret-du-18-mars-2015/ [consulté le 21/08/2018]

- TA Paris, 5e section, 2e chambre, n°1508951/5-2, 18 Février 2016, C+

2) Conseil de l'Europe

- Convention européenne des droits de l'homme, telle qu'amendée par les Protocoles n°11 et 14, complétée par le Protocole additionnel et les Protocoles n°4, 6, 7, 12 et 13

3) Droit de l'UE

- 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, Article 12

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

- Charte des droits fondamentaux de l'Union européenne, JOUE n°202 C du 7 Juin 2016, p. 389-405

4) Italie

- DECRETO LEGISLATIVO 7 marzo 2005, n. 82 (modifié par le Decreto Legislativo 13 dicembre 2017, n. 217), Codice dell'amministrazione digitale. (GU n.112 del 16-5-2005-Suppl. Ordinario n.93). Disponible sur : http://www.normattiva.it/showNewsDetail;jsessionid=aPCShq+pDnWUpDf0goto6g__.na1-prd-norm?id=987&backTo=evidenza [consulté le 20/08/2018]

5) Bulgarie

- Loi sur la gouvernance électronique, 13 juin 2008 (dernière modification le 9 décembre 2016) (ЗАКОН ЗА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ, В сила от 13.06.2008 г) Disponible sur : https://lex.bg/index.php/laws/ldoc/2135555445 [consulté le : 20/08/2018]

B) Actes non contraignants

1) France

Rapports

- Commission Informatique et libertés. *Rapport de la Commission informatique et libertés.* Paris : La documentation française, 1975. 106 p.

- Rapport d'information de MM. Alain ANZIANI et Antoine LEFÈVRE, fait au nom de la commission des lois, n° 445 (2013-2014) - 9 avril 2014

- *Conseil d'État, Le numérique et les droits fondamentaux, Étude* annuelle 2014, *Études et documents, Conseil d'État,* n°65. Paris : La documentation française, 2014. 448 p.

- Conseil National du Numérique. *Rapport Jules Ferry 3.0. Bâtir une école créative et juste dans un monde numérique.* Octobre 2014. 118 p.

- Commission nationale de l'informatique et des libertés. *Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle. Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique,* Décembre 2017. 75 p.

- Cour des comptes, *Rapport public annuel 2018*, Février 2018.

Avis de la CADA

- CADA, avis n° 20144578 du 8 janvier 2015

- CADA, avis n°20161989 du 23 juin 2016

Délibérations de la CNIL

- CNIL. Délibération n°03-036 du 1 juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

- CNIL. Délibération n° 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

Autre

- Plan d'action national 2018-2020 de la France dans le cadre du Partenariat pour un gouvernement ouvert. Disponible sur : https://www.etalab.gouv.fr/wp-content/uploads/2017/03/20180503_France-national-action-plan-2018-2020-EN.pdf [consulté le 14/08/2018]

2) Union Européenne

- Commission européenne. « Une approche européenne en matière d'intelligence artificielle ». *Questions et réponses.* Bruxelles, le 25 avril 2018

3) Conseil de l'Europe

- Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique (adoptée par le Comité des Ministres le 30 septembre 2004, lors de la 898e réunion des Délégués des Ministres)

- Recommandation CM/Rec(2017)5[1] du Comité des Ministres aux États membres sur les normes relatives au vote électronique (adoptée par le Comité des Ministres le 14 juin 2017, lors de la 1289e réunion des Délégués des Ministres)

- Lignes directrices pour la mise en œuvre des dispositions de la Recommandation CM/Rec(2017)5 sur les normes relatives au vote électronique

II) Documentation non officielle

1) Thèses

- CHILOWICZ Michel. Recherche de similarité dans du code source. ROUSSEL Gilles (dir. De Recherche). Thèse de doctorat. Informatique. Université Paris-Est. 2010. 280 p. Disponible sur : https://pastel.archives-ouvertes.fr/tel-00587628/document [consulté le 7/08/2018]

- MODESTE Simon. *Enseigner l'algorithme pour quoi ? Quelles nouvelles questions pour les mathématiques ? Quels apports pour l'apprentissage de la preuve ?.* GRAVIER Sylvain (dir. De Recherche). Thèse de doctorat. Mathématiques-informatique. Université de Grenoble, 2012. 255 p. Disponible sur : https://tel.archives-ouvertes.fr/tel-00783294/document [consulté le 7 août 2018]

2) Ouvrages généraux

- AMINI Massih-Rezah. *Apprentissage machine : de la théorie à la pratique*. Paris : Editions Eyrolles, 2015. 293 p.

- KNUTH Donald. *Selected papers on computer science.* Center for the Study of Language and Information, 1996. 276 p. Disponible sur : https://doc.lagout.org/science/0_Computer%20Science/7_Technical%20Papers/Selected%20Papers%20on%20Computer%20Science%20-%20Donald%20E.%20Knuth.pdf [consulté le 9/08/2018]

- LAFARGUE France. *Dictionnaire français/anglais de l'informatique. AFNOR,* 2003. 483 p.

- LILEN Henri. *Dictionnaire informatique et numérique.* Paris : Editions First-Gründ, 2011. 254 p.

3) Monographies

- BOURCIER Danièle (dir.), DE FILIPPI Primavera (dir.). *Open Data & Big Data: Nouveaux défis pour la vie privée.* Editions mare&martin, 2016. 269 p.

- FOREY Elsa (dir.), GESLOT Christophe (dir.). *Internet, machines à voter et démocratie*. Paris : L'Harmattan, 2011. 235 p.

- GUGLIELMI Gilles (dir.), IHL Olivier (dir.). *Le vote électronique*. LGDJ, 2015. 323 p.

- KERSTING Norbert, BALDERSHEIM Harald. *Electronic Voting and Democracy : A comparative Analysis*. Palgrave Macmillan, 2004. 309 p.

- KOUBI Geneviève (dir.), CLUZEL-MÉTAYER Lucie (dir.), TAMZINI Wafa (dir.). *Lectures critiques du Code des relations entre le public et l'administration*. LGDJ, 2018. 229 p.

4) Actes de colloque

- GUGLIELMI Gilles (dir.), ZOLLER Elizabeth (dir.). *Transparence, démocratie et gouvernance citoyenne. Colloque international des 23 et 24 mai 2014.* Paris : Éditions Panthéon-Assas, 2014. 257 p.

- IFSA, CADA. *Transparence et secret. Colloque pour le XXVe anniversaire de la loi du 17 juillet 1978 sur l'accès aux documents administratifs.* Paris : La documentation française, 2004. 334 p.

- LE BOT Olivier (dir.), ARLETTAZ Jordane (dir.). *La démocratie en un clic ? Réflexions autour de la notion d'e-démocratie. Actes du colloque de Nice – 16 novembre 2009*. Paris : L'Harmattan, 2010. 129 p.

- MARCHAND Jennifer. « L'accès et la réutilisation des données publiques dans le cadre de la loi pour une République numérique ». *In :* CHATRY Sylvain (dir.), GOBERT Thierry (dir.). *Numérique : nouveaux droits, nouveaux usages. Actes de colloque.* Editions mare&martin, 2017. 280 p.

5) Articles de revue

- ALGAN Yann, Maya BACACHE-BEAUVALLE, PERROT Anne. « Administration numérique », *Notes du conseil d'analyse économique*, 2016/7 (n° 34). p. 1-12

- AUBY Jean-Bernard. « Le droit administratif face aux défis du numérique ». *AJDA,* 2018. p. 835

- BIRCH Sarah, COCKSHOTT Paul, RENAUD Karen. « Putting Electronic Voting under the Microscope ». *The Political Quaterly*, vol. 85, n°2, April-June 2014. p. 187-194. Disponible sur : https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-923X.12071 [consulté le 17/07/2018]

- ENGUEHARD Chantal. « Le vote électronique en France. Opaque et vérifiable ». *Legalis.net*, décembre 2006, n°4, p. 83-97

- ENGUEHARD Chantal. « Le vote électronique est-il transparent, sûr, fiable ? ». *Science et pseudo-Sciences*, n°320, avril 2017. Disponible sur : http://www.pseudo-sciences.org/spip.php?article2800 [consulté le 3 août 2018]

- FOREST David. « La régulation des algorithmes, entre éthique et droit ». *Revue Lamy Droit de l'Immatériel*, n°137, 1er mai 2017. p. 1-15. Disponible sur : www.lamyline.fr [consulté le 16/02/2018]

- FOUTEL Nathalie. « Licences libres en secteur industriel sensible : un usage stratégique », *Revue Droit de l'Immatériel*, n°77, 1er décembre 2011. Disponible sur : www.lamyline.fr [consulté le 16/02/2018]

- GHEVONTIAN Richard. « La notion de sincérité du scrutin ». *Cahiers du Conseil Constitutionnel*, n°13, Dossier : la sincérité du scrutin, Janvier 2003. Disponible sur : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/la-notion-de-sincerite-du-scrutin [consulté le : 3 août 2018]

- GICQUEL Jean-Eric. « Le vote électronique en France ». *Petites affiches*, n°68. p. 5. Disponible sur : https://www.lextenso.fr/ [consulté le 18/07/2018]

- GICQUEL Jean-Eric. « Le vote par Internet : une modalité électorale à aborder avec circonspection ». *La semaine juridique – Éditions administrations et collectivités territoriales*, n°31-35, 31 juillet 2006. p. 1091-1094

- GOODMAN Bryce, FLAYMAN Seth. « European Union regulations on algorithmic decision-making and a ' right to explanation ' ». *AI Magazine*, Vol 38, No 3, 2017. p. 1-9. Disponible sur : https://arxiv.org/abs/1606.08813 [consulté le 27/05/2018]

- KOUBI Geneviève. « Les machines à voter en questions… parlementaires ». *Revue du droit public*, n°1, Janvier 2014. p. 101. Disponible sur : https://www.lextenso.fr/ [consulté le 18/07/2018]

- LESSIG Lawrence. « Code is law. On liberty in Cyberspace ». *Harvard Magazine*, janvier 2000. 5 p. Disponible sur : https://harvardmagazine.com/2000/01/code-is-law-html [consulté le 22/08/2018]

- SCHURR Ludovic. « Logiciel libre : un panorama des évolutions jurisprudentielles et politiques publiques ». Revue Le Lamy Droit de l'immatériel, Nº 102, 1er mars 2014. Disponible sur : www.lamyline.fr [consulté le 16/02/2018]

- SILGUY Stéphanie De. « Doit-on se méfier davantage des algorithmes ? ». *Revue Lamy Droit civil*, n°146, 1er mars 2017. p. 1-10. Disponible sur : www.lamyline.fr [consulté le 16/02/2018].

- SURDEN Harry. « Values Embedded in Legal Artificial Intelligence ». *U of Colorado Law Legal Studies Research Paper*, n°17-17, 15 mars 2017. p. 1-6. Disponible sur :https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2932333 [consulté le 22/08/2018]

- VALAT Grimaud. « Propositions pour un encadrement du régime juridique des logiciels ». *Revue Le Lamy Droit de l'Immatériel,* n°123, 1er février 2016. p. 1-7. Disponible sur www.lamyline.fr [consulté le 15/02/2018]

6) Sites Internet

- Commission européenne. « European Union Public License ». Disponible sur : https://ec.europa.eu/info/node/2820 [consulté le 15/08/2018]

- Commission européenne. « Open source software strategy ». Disponible sur : https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en#opensourcesoftwarestrategy [consulté le 15/08/2018]

- Commission européenne. « Open Source Strategy : History ». Disponible sur : https://ec.europa.eu/info/open-source-strategy-history_en [consulté le 15/08/2018]

- Free Software Foundation Europe. « Public Money ? Public Code ! ». Disponible sur : https://fsfe.org/campaigns/publiccode/publiccode.fr.html [consulté le 16/08/2018]

- Free Software Foundation, « Qu'est-ce que le logiciel libre ? ». Disponible sur : https://www.gnu.org/philosophy/free-sw.fr.html [consulté le 7/08/2018]

- Free Software Foundation. « Catégories de logiciels libres et non libres ». Disponible sur https://www.gnu.org/philosophy/categories.html [consulté le 11/08/2018]

- http://references.modernisation.gouv.fr/socle-logiciels-libres [consulté le 14/08/2018]

- https://publiccode.eu/ [consulté le 16/08/2018]

- Le blog d'Etalab. « Le Partenariat pour un gouvernement ouvert (« PGO », ou Open Government Partnership – « OGP ») ». Disponible sur : https://www.etalab.gouv.fr/ogp [consulté le 14/08/2018]

- Open Government Partnership. « Mission and Strategy ». Disponible sur : https://www.opengovpartnership.org/mission-and-strategy [consulté le 14/08/2018]

7) Articles non scientifiques

- « Développement de l'administration électronique : où en est-on ? ». *Vie-publique.fr,* 7 avril 2005. Disponible sur http://www.vie-publique.fr/actualite/dossier/administration-electronique-2005/developpement-administration-electronique-ou-est-on.html [consulté le 27/08/2018]

- ANGWIN Julia, LARSON Jeff, MATTU Surya, KIRCHNER Lauren. « Machine Bias. There's software used across the country to predict future criminals. And it's biased against black ». *Propublica.org,* 23 mai 2016. Disponible sur : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [consulté le 25/08/2018]

- BOZHANOV Bozhidar. « Bulgaria Got a Law Requiring Open Source ». *Thepolicy.us*, 4 Juillet 2016. Disponible sur : https://thepolicy.us/bulgaria-got-a-law-requiring-open-source-98bf626cf70a [consulté le 20/08/2018]

- Free Software Foundation Europe. « "Public Money? Public Code!": plus de traductions, plus de soutiens, plus de sensibilisation ». 26 Juillet 2018. Disponible sur : https://fsfe.org/news/2018/news-20180725-01.fr.html [consulté le 16/08/2018]

- Info Barcelona. « Barcelona's Digital Government: Open, Agile and Participatory ». 20 octobre 2017 Disponible sur : https://www.barcelona.cat/infobarcelona/en/barcelonas-digital-government-open-agile-and-particpatory_565416.html [consulté le 16/08/2018]

- MARZIN Jacques. « L'État plateforme donnera naissance à de nouveaux services publics numériques ». 17 septembre 2015. Disponible sur : http://www.modernisation.gouv.fr/ladministration-change-avec-le-numerique/par-son-systeme-dinformation/etat-plateforme-tribune-marzin [consulté le 20 août 2018]

- SHENOY Navin. « Intel security issue update : addressing reboot issues ». Intel Newsroom, 11 Janvier 2018. Disponible sur : https://newsroom.intel.com/news/intel-security-issue-update-addressing-reboot-issues/ [consulté le 20/08/2018]

- SHENOY Navin. « Root cause of reboot issue identified ; updates guidance for customers and partners ». Intel Newsroom, 22 janvier 2018. Disponible sur : https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners/ [consulté le 20/08/2018]

8) Autre

- « Preisdent Obama asks America to learn computer science ». https://www.youtube.com/watch?v=6XvmhE1J9PY [consulté le 26/08/2018]

- « President Obama meets with students at an Hour of Code Event ». https://www.youtube.com/watch?v=EJEBGf_uS_M [consulté le 26/08/2018]

- « En 2016, le code informatique arrive à l'école ». *LeMonde.fr*, 2 novembre 2016. Disponible sur : https://www.lemonde.fr/sciences/article/2016/11/02/en-2016-le-code-informatique-arrive-a-l-ecole_5024344_1650684.html [consulté le 26/08/2018]

- Déclaration de M. François Hollande, Président de la République, sur le numérique à l'école, à Paris le 16 décembre 2016. Disponible sur : http://discours.vie-publique.fr/notices/167003770.html [consulté le 26/08/2018]

- LE NEVÉ Soazig. « Parcoursup : ouverture des inscriptions sous haute tension ». L*eMonde.fr,* 22 janvier 2018. Disponible sur : https://www.lemonde.fr/campus/article/2018/01/22/parcoursup-ouverture-des-inscriptions-sous-haute-tension_5245273_4401467.html [consulté le 26/08/2018]

- VIDAL Frédérique. « Parcoursup : publication du code informatique des algorithmes ». [communiqué]. Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation, 21 mai 2018. Disponible sur : http://m.enseignementsup-recherche.gouv.fr/cid130453/parcoursup-publication-du-code-informatique-des-algorithmes.html [consulté le 26/08/2018]

- MAHJOUBI Mounir (@mounir). « Avec @VidalFrederique, on l'a dit, on le fait ! Aujourd'hui nous rendons public 100% du code source de #Parcoursup et sa documentation scientifique. Notre engagement : garantir la transparence des algorithmes publics ». Twitter, 21 mai 2018, https://twitter.com/mounir/status/998524796307587072 [consulté le 26/08/2018]

Table des matières