Les Systèmes Inéquitables Numériques (SIN)

Chantal Enguehard
LS2N, UMR CNRS 6004, Université de Nantes
2, rue de la Houssinière - BP 92208 - 44322 Nantes Cedex 03

Anaïs Danet
Professeure en droit privé et sciences criminelles, CEJESCO EA 4693, Université de Reims Champagne Ardenne
Campus Croix-Rouge – Avenue François Mauriac -CS 40019–51 726 Reims Cedex

Résumé

Le développement des applications numériques entraîne une multiplication des interactions numériques, d'ailleurs parfois imposées aux usagers. Malheureusement, ces applications sont susceptibles de dysfonctionner. Ce sont ces dysfonctionnements et plus particulièrement leurs conséquences que cette étude entend appréhender.

Nos observations croisées de juriste et d'informaticienne nous ont amenées à mettre en lumière l'existence de Systèmes Inéquitables Numériques (SIN), dispositifs numériques intervenant dans une relation juridique entre deux sujets de droit et dont les traces pourraient être utilisées comme éléments de preuve de l'exécution ou de l'inexécution d'une obligation.

Mais, lorsqu'un litige survient, toutes les parties n'ont pas accès aux traces témoignant de l'(in)exécution des obligations juridiques. Nous étudions comment rétablir l'équilibre entre les parties par exemple en donnant un égal accès aux traces numériques (la fiabilité de ces traces doit alors être interrogée). Il apparaît que ces difficultés pourraient être anticipées dès la conception des systèmes numériques et leur identification en tant que SIN.

Mots-clefs

Droit, numérique, SIN, Système inéquitable numérique, trace probante

1 Introduction

Dans notre société, le numérique s'immisce dans une grande partie des rapports sociaux : vie quotidienne, vie professionnelle, vie politique (citoyenneté), vie scolaire ou estudiantine, etc. Des systèmes numériques réalisent l'enregistrement d'informations, leur transformation, leur transmission ou encore leur publication. Or ces systèmes numériques sont susceptibles de connaître des dysfonctionnements tels une indisponibilité, l'enregistrement incomplet d'une information, la modification erronée d'une information, une perte d'informations, etc. L'origine de ces dysfonctionnements peut être attribuée à la présence de bugs de conception ou de développement, à des virus

malveillants ou encore des erreurs d'exécution dues, par exemple, aux rayonnements cosmiques.[1]

Il est nécessaire de commencer par proposer une définition des systèmes inéquitables numériques. Pour ce faire, il faut revenir sur le concept d'inéquité à travers celui d'équité, avant de confronter ce concept aux systèmes numériques.

2 L'équité

Les juristes ont davantage tendance à définir l'équité que l'inéquité, l'équité étant d'ailleurs elle-même une notion fuyante. Issue du latin « *aequitas* », ayant la même racine qu'« *aequus* » qui signifie « égal », l'équité peut emprunter deux sens selon qu'il s'agit d'équité substantielle ou processuelle :

L'**équité substantielle** renvoie à la valeur qui permet au juge de corriger ou de compléter le droit lorsque les solutions résultant de son application stricte sont injustes. L'idée est que le juge doit « *peser les intérêts en présence afin de les rééquilibrer, de les égaliser au sens de l'égalité proportionnelle* » [2].

L'**équité processuelle** convoque le concept globalisant de « procès équitable », tel que protégé par l'article 6 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, qui renvoie schématiquement à l'idée que, pour qu'un procès soit équitable, les parties doivent être traitées sur un pied d'égalité. On remarque d'ailleurs que le respect de l'équité processuelle implique l'impartialité du juge, qui doit se trouver à « *égale distance* » de chacune des parties, ainsi que le respect de *l'égalité des armes*, et fait également écho au principe du contradictoire qui permet à toutes les parties d'avoir accès aux mêmes informations.

3 Système Inéquitable Numérique

3.1 Système Numérique

Nous définissons un **système numérique** comme un assemblage de différents composants : numériques (logiciels, système d'exploitation, réseau), matériels (ordinateur, ordiphone, lecteur de carte, distributeur de tickets), auxquels il faut ajouter l'organisation humaine qui l'entoure et qui en assure le fonctionnement (mises à jour logicielles, dépannage, etc.).

Différents sujets de droit interviennent lors de l'usage d'un système numérique. *A minima* l'utilisateur d'une part et le détenteur/responsable/propriétaire du système numérique d'autre part.

Il arrive que des systèmes numériques soient utilisés notamment pour matérialiser l'exécution d'une obligation juridique et, par suite, pour l'enregistrer. Or, l'utilisation d'un système numérique comme source de preuve de l'exécution de cette obligation peut engendrer plusieurs types de difficultés, la première étant que le système numérique est bien souvent mis en place, géré et contrôlé par une seule des deux parties

1. Les flux de particules venus du cosmos sont capables de traverser murs et blindages et de perturber le fonctionnement des microprocesseurs des ordinateurs [3].

en cause. Dans cette configuration, apparaît donc une inégalité entre les différents acteurs du système numérique. Voilà pourquoi il est possible de parler à leur égard de **Systèmes Inéquitables Numériques** ou **SIN**.

3.2 Dysfonctionnements numériques

Depuis plusieurs années, des cas de dysfonctionnements de systèmes numériques ayant eu un impact sur les usagers sont constatés. En voici quelques exemples :

- dès 2012 : des litiges de consommation apparaissent avec des vélos en libre-service [5] ;
- en 2013 : des personnes sont privées de sécurité sociale[2] ;
- en 2014 : des usagers de tickets de transports électroniques ne peuvent valider leur ticket électronique et voyagent illégalement[3] ;
- en 2014 : des devoirs déposés par des étudiants disparaissent d'une plate-forme de dépôt universitaire[4] ;
- en 2017 : une électrice genevoise se voit reprocher un mauvais comportement après avoir tenté, sans succès, de voter par internet[5] ;
- en 2018 : une femme attend pendant quatre mois la délivrance de son permis de conduire du fait d'une défaillance de l'Agence nationale des titres sécurisés. Cette femme ne peut honorer son travail de chauffeur de bus scolaire ce qui met aussi son entreprise en difficulté[6] ;
- en 2018 : Plusieurs États indiens généralisent l'usage du système Aadhaar indispensable pour se marier, ouvrir un compte en banque, accéder à ses droits sociaux (y compris l'obtention de rations de survie en cas de famine) ou acheter un téléphone cellulaire. Or, l'identification biométrique des empreintes digitales qui lui est associée échoue à reconnaître certaines personnes ce qui les prive de ces droits[7] ;
- en 2019 : des usagers d'Android sont abonnés à des services payants à leur insu[8].

Les causes sont multiples : il peut s'agir de limites inhérentes aux techniques utilisées (reconnaissance biométrique), de bugs non identifiés avant déploiement, de manœuvres délictueuses (virus, piratage), ou encore de causes non identifiées.

Le préjudice des usagers peut prendre différentes formes : contrainte à agir illégalement (cas des tickets de transport), perte monétaire en cas d'achat forcé, mise en doute de la réputation d'honnêteté (cas du vote électronique à Genève), mauvaise notation

2. Aires, Gwendolen. "Sans Sécu à leur insu", Libération, 12 sept 2013.

3. Presse Océan. "Nantes Transports : Un bug sur « mTicket". 20 octobre 2014.

4. Observation personnelle.

5. Tribune de Genève. "Après un vote raté sur Internet, une citoyenne écope d'un avertissement", 21 février 2017.

6. Ouest France. "Pas de permis : Véronique ronge son frein", 27 mai 2018

7. Frayer, Lauren. Latif Khan, Furkan. Myers, India's Biometric ID System Has Led To Starvation For Some Poor, Advocates Say, NPR (National Public Radio), 1er oct 2018.

8. 20 minutes, "Google : Un virus abonne ses victimes à des services payants sans leur consentement", 11 septembre 2019.

(étudiants), privation de droits spécifiques (à la sécurité sociale, à l'emploi) ou encore à de multiples droits comme en Inde.

Nous focalisons notre attention sur les cas pour lesquels :

- l'usager rencontre des difficultés à prouver sa bonne foi ;
- les acteurs (usager d'une part / société d'autre part) ont une position asymétrique quant à l'accès aux traces numériques des interactions qui ont eu lieu.

Voici des exemples de SIN.

Le service de **location de vélo** de Nantes Métropole est bicloo[9] de la société Cyclocity, opératrice du groupe JCDecaux. Les informations affichées sur le site web[10] indiquent : « *Lorsque vous déposez votre vélo attendez quelques minutes, un signal sonore et un voyant lumineux vous confirment que votre vélo est bien verrouillé.* ». Ces traces, sonores et lumineuses, sont fugitives au sens où l'utilisateur ne peut les conserver pour ensuite les produire à titre de preuve. Par ailleurs, lorsqu'un vélo n'est pas retourné sur une borne de location, le compte bancaire du client est débité d'une somme de 150 euros (montant du dépôt de garantie). Or, il peut arriver que le système de raccrochage fonctionne mal, ce qui aboutit à libérer un vélo, entraînant une pénalité de 150 euros pour le dernier client alors même qu'il ne peut produire une preuve de sa bonne remise du vélo. En 2014, le motif le plus courant de saisine du médiateur de JCDecaux a été la demande de remboursement de cette pénalité de 150 euros[11].

La Société d'économie mixte des transports en commun de l'agglomération nantaise (SEMITAN) est l'exploitant du réseau de transport en commun de Nantes Métropole. **Des titres de transports dématérialisés** ont fait leur apparition sous deux formes. La première forme est une carte à puce nommée **LiberTan** qui peut héberger, entre autres, des tickets à l'unité donnant le droit de voyager durant une heure. Pour valider son titre de transport, l'usager passe sa carte devant une des bornes de validation. La borne émet alors un son et affiche un message, mais l'usager ne dispose d'aucune trace tangible de la validation de son ticket de transport. Cette situation contraste avec la validation d'un ticket cartonné sur lequel l'usager peut constater, lui-même, sans intermédiaire logiciel ou matériel, que l'horodatage de sa validation a été inscrit sur le ticket et qu'il est lisible.

Lors d'un contrôle de la validité des titres de transport, le contrôleur procède *via* des outils numériques. Un usager peut se voir contester la validation de son titre de transport qu'il a pourtant bien effectuée si celle-ci a été mal enregistrée, si l'enregistrement a disparu, ou encore s'il n'est pas accessible. Dans ce cas, il se voit infliger une amende : en l'absence de trace tangible, l'usager ne dispose d'aucun élément pour prouver sa bonne foi. Par ailleurs, d'autres dysfonctionnements lésant l'usager peuvent subvenir, comme la validation non souhaitée de plusieurs titres de transport.

9. http://www.bicloo.nantesmetropole.fr - Consulté le 3 décembre 2017

10. http://www.bicloo.nantesmetropole.fr/Comment-ca-marche/Les-stations/Les-points-d-attache - Consulté le 3 décembre 2017.

11. Rapport du Médiateur 2014 VLS France JCDecaux.

4 Qualification de systèmes inéquitables numériques

Dans le cas du vélo en libre-service ou de la carte de transport, l'inéquité qui permet de qualifier ces dispositifs de SIN trouve sa source dans l'asymétrie d'information. En effet la disponibilité de la « trace » résultant de l'utilisation est différente pour l'utilisateur ou la société utilisant les serveurs d'enregistrement des informations.

C'est donc une forme d'inéquité processuelle qui peut être convoquée en ce qui concerne les systèmes inéquitables numériques, les parties n'étant pas placées sur un pied d'égalité. Les systèmes inéquitables numériques décrits plus hauts sont inéquitables précisément parce qu'ils ne placent pas les **personnes en interaction avec lui** (consommateur, usager, société) sur un pied d'égalité, en avantageant certains, le plus souvent les professionnels, au détriment des autres.

Les SIN sont par conséquent susceptibles de générer des difficultés sur le plan juridique, et plus précisément sur le plan de la preuve, lorsque leur utilisation correspond matériellement à l'exécution d'une obligation juridique. En effet, la question de la preuve de l'exécution de cette obligation ou de son inexécution est susceptible de se poser, *a fortiori* si le système est défaillant.

D'où la question de savoir **comment le droit de la preuve judiciaire appréhende ces systèmes inéquitables numériques.**

La question est d'autant plus intéressante que ces systèmes sont relativement récents et tendent à se développer, alors que le contentieux nourri par ces SIN est quasi-invisible. En effet, il s'agit principalement de petits litiges, qui n'entraîneront pas nécessairement la saisine d'un tiers pour le régler, le coût de la procédure étant bien souvent supérieur au montant du litige. En outre, quand bien même la partie lésée irait contester la fiabilité du SIN, le contentieux sera réglé le plus souvent par un processus amiable de règlement des litiges. Le développement des préalables de conciliation obligatoire pour le règlement des petits litiges, encore accentué par la loi du 23 mars 2019[12], conduira ainsi à la résolution extra-judiciaire de ces éventuels litiges liés à des SIN. D'ailleurs, les quelques litiges relatifs au raccrochage des Velib à Paris ayant donné lieu à la saisine du Tribunal d'Instance de Courbevoie se sont soldés par une médiation réussie entre l'exploitant JCDecaux et les utilisateurs qui affirmaient avoir correctement raccroché leur vélo à la borne. Le recours à la médiation ne permet ainsi pas d'apprécier véritablement la façon dont le droit appréhende les preuves issues des SIN, pas plus que de percevoir la difficulté de les obtenir. Finalement, trop peu de décisions de justice tranchent ce type de litige pour pouvoir en tirer des conclusions pertinentes. A notre connaissance, un seul litige a donné lieu à une décision du Tribunal d'instance de Toulouse, lequel s'est prononcé en faveur des utilisateurs du vélo en libre-service de la ville[13].

La quasi-invisibilité du contentieux lié à l'utilisation des SIN ne doit pourtant pas conduire à nier l'existence de ces difficultés, susceptibles de toucher un public très

12. Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, réformant, en son article 3, l'article 4 de la loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle.

13. Cette décision de justice est de surcroît inaccessible sur les bases de données juridiques ; seule la presse locale s'en est fait l'écho…

large. Notre intention est donc en premier lieu de comprendre quelles sont les difficultés créées par les systèmes inéquitables numériques dans le droit de la preuve (4.1) pour tenter en second lieu de proposer des pistes pour les résoudre ou, mieux, s'en prémunir (4.2).

4.1 Les SIN créateurs de difficultés dans le droit de la preuve

En premier lieu, il est nécessaire d'identifier les difficultés engendrées par les systèmes inéquitables numériques au regard du **droit de la preuve**. Ces difficultés sont en réalité de deux ordres. D'une part, les SIN engendrent des obstacles théoriques au droit à la preuve parce qu'ils compliquent l'accès à la preuve (4.1.1). D'autre part, à supposer que l'on puisse y avoir accès, la confiance portée aux systèmes numériques complexifie d'autant leur remise en question par le justiciable, de telle sorte qu'il existerait une distorsion entre la valeur juridique d'une telle preuve et son impact réel sur l'issue du litige (4.1.2).

4.1.1 Difficulté d'accéder à la preuve numérique issue d'un SIN

Le droit à la preuve peut se définir comme « *le pouvoir d'exiger du juge qu'il accueille l'offre ou la demande de preuve présentant un caractère licite et pertinent* » [1]. Ainsi, lorsqu'une partie ne peut avoir accès par elle-même à un élément de preuve qu'elle sait exister, il devrait lui être possible de solliciter le concours du juge notamment pour obtenir cet élément de preuve grâce à une mesure d'instruction. Il faudrait donc en théorie pouvoir rechercher cette preuve dans le système inéquitable numérique.

Ici des difficultés techniques apparaissent.

D'abord, il est difficile de prévoir à l'avance quelle information sera nécessaire pour résoudre un litige et le système numérique n'enregistre pas nécessairement toutes les informations parmi la multitude qu'il pourrait avoir à enregistrer (date, heure, lieu, numéro de la carte bancaire ayant effectué le paiement, numéro du vélo, numéro du plot auquel a été rattaché le vélo, etc.). Il est donc possible que la preuve n'existe tout simplement pas.

Ensuite, pour qu'une information numérique devienne une **preuve numérique**, il est nécessaire qu'elle respecte trois critères que sont l'authenticité, l'intégrité et la traçabilité [4]. En effet, l'**authenticité** garantit l'origine de l'information, l'**intégrité** garantit son contenu et la **traçabilité** garantit la façon dont cette preuve a été copiée[14]. Or, en matière de systèmes inéquitables numériques, et à supposer que les données utiles soient correctement enregistrées, il est difficile de s'assurer que celles-ci ont été correctement conservées sans modification. S'il existe des normes de conservation particulières relatives aux données personnelles, il n'est pas certain que l'ensemble des données enregistrées par le système puissent être qualifiées comme telles. En effet, s'il est vrai que les données enregistrées contiennent nécessairement des données personnelles, faute de quoi elles ne seraient pas utilisables, à défaut de pouvoir identifier l'emprunteur du vélo ou l'utilisateur des transports publics, toutes les données utiles à la solution du litige ne sont pas nécessairement des données personnelles – il en va ainsi par exemple de l'heure à laquelle le vélo a été raccroché, par exemple. Il n'est par

14. *Ibid*, spéc. p. 22 et s.

conséquent pas certain que ces données non-personnelles puissent bénéficier de la protection de ces normes de conservation. Par conséquent, il serait utile que des normes similaires s'appliquent à toutes les données enregistrées lors du service (location de vélo, validation d'un ticket de transport) afin de garantir l'intégrité desdites données.

Enfin, et de façon plus pragmatique, le prestataire n'a *a priori* aucune obligation de répondre gracieusement aux demandes d'accès aux traces numériques de ses systèmes, puisqu'il ne s'agit pas à proprement parler de « données personnelles ». L'accès aux traces numériques nécessitera alors de mandater un expert, dont le coût serait très vraisemblablement supporté par la personne qui sollicite cette expertise. En effet, si l'article 269 du Code de procédure civile prévoit que le juge peut mettre à la charge de l'une ou l'autre des parties ou des deux la consignation de la provision à valoir sur la rémunération de l'expert, le demandeur à la mesure d'expertise est, la plupart du temps, désigné pour consigner cette provision. En effet, l'article 271 du Code de procédure civile prévoit, qu'en principe, à défaut de consignation dans le délai imparti, la désignation de l'expert est caduque : par conséquent, pour éviter que le défendeur à la demande d'expertise ne paralyse la procédure en ne payant pas la consignation, c'est sur la tête du demandeur que reposera cette consignation dans la grande majorité des cas . Cette répartition initiale du coût de l'expertise vient entraver, au moins matériellement l'accès aux preuves issues des systèmes inéquitables numériques, d'autant qu'il s'agit là de montants élevés puisque ces expertises sont coûteuses et que le montant de la consignation doit être aussi proche que possible de la rémunération définitive prévisible[15].

4.1.2 Difficulté de contester la preuve numérique issue des SIN

A supposer qu'une preuve soit accessible et puisse être utilisée, il faut s'interroger sur sa valeur et sur la possibilité dont pourrait disposer les parties de contester cette preuve. Or, il existe une véritable distorsion entre la valeur théorique d'une preuve et son impact réel sur l'issue d'un litige.

En effet, théoriquement, cette trace numérique correspond à un code, qui est nécessairement intelligible soit directement (si, par exemple, la trace indique clairement « retrait le 12/10/2016 à 16h03 »), soit indirectement parce qu'elle a été chiffrée – mais dans cette hypothèse il est toujours possible de la dé-chiffrer grâce à la clé numérique adéquate. Par conséquent, cette trace numérique peut être qualifiée d'écrit au sens de l'article 1365 du Code civil qui dispose que « *l'écrit consiste en une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quel que soit leur support* ». Toutefois, au regard de la classification des modes de preuve proposée par le Code civil, il ne s'agit à l'évidence ni d'un acte authentique ni même d'un acte sous seing privé. Cet écrit devrait alors être analysé tout au plus comme un « indice » susceptible de constituer une présomption au sens de l'article 1382 du Code civil. La valeur probante de ces présomptions est alors laissée à la libre appréciation du juge et il est en principe possible de les renverser.

Pourtant, et on touche là aux confins de la psychologie, la confiance dans le numérique est extrêmement solide, à tel point qu'elle est d'ailleurs un véritable objectif politique affiché dans les lois de ces dernières années « *pour la confiance dans l'économie*

15. Art. 269 *C. proc. civ.*

numérique »[16], ou encore « *pour une république numérique* »[17]. Cette confiance est telle que la preuve numérique sera vraisemblablement jugée plus fiable qu'un témoignage et qu'il sera difficile de la contester. En réalité, pour être fiable, une trace numérique doit être signée numériquement (c'est-à-dire chiffrée) pour garantir qu'elle n'est pas volontairement modifiée et rien ne garantit à l'heure actuelle que les systèmes inéquitables numériques signent numériquement leurs traces numériques. En outre, le système n'est, quoi qu'il arrive, pas à l'abri d'un bug qu'il pourra être extrêmement difficile de prouver.

Nous avons démontré que les systèmes inéquitables numériques sont loin d'être anodins sur le plan de la preuve. Il est donc nécessaire de chercher à proposer des solutions pour résoudre ces difficultés, ou mieux, les faire disparaître. C'est l'objet de notre seconde partie.

4.2 Le droit de la preuve, source limitée de solutions aux difficultés créées par les SIN

En second lieu, il nous appartient de chercher des solutions pour minimiser ces difficultés. Plusieurs pistes peuvent alors être proposées, qui sont plus ou moins pertinentes. L'hypothèse est la suivante : un voyageur en transport en commun doit valider son titre de transport numérique sur une borne prévue à cet effet. Toutefois, un litige survient : il affirme avoir validé correctement son titre de transport alors que le système semble *a priori* n'en avoir gardé aucune trace. Toute la difficulté réside dans la nécessité de prouver l'utilisation conforme du système et donc de prouver qu'il y a eu ou non un dysfonctionnement du système numérique. En théorie, pour prouver l'existence ou l'inexistence d'un dysfonctionnement, une expertise est possible. Mais cette solution intervenant *a posteriori* n'est que peu pertinente car difficile à mettre en œuvre (4.2.1). Il serait par conséquent plus opportun de chercher à prévenir ces difficultés (4.2.2).

4.2.1 La résolution *a posteriori* des difficultés peu opportune

Résoudre les difficultés probatoires posées par les systèmes inéquitables numériques impliquerait de pouvoir recourir à une expertise capable de démontrer qu'un bug existe et d'en préciser la portée.

Il est alors envisageable de demander au juge d'avoir copie des traces d'usages ou de mandater un expert afin que ce dernier accède aux traces d'usage.

Or un prestataire ne peut garder trace de tous les traitements d'information effectivement réalisés car la quantité d'informations serait pléthorique. Il doit donc forcément effectuer une sélection en décidant la nature des traces conservées et la durée de leur conservation. Il est donc possible qu'un bug ne soit pas perceptible par l'analyse des traces effectivement conservées par le prestataire. De plus, les traces d'usage sont elles-mêmes sujettes à caution. Techniquement, pour déterminer dans quelle mesure elles reflètent l'usage véritable, il est nécessaire que l'expert évalue la sûreté de la chaîne d'horodatage et de signature numérique et qu'il détermine si des incidents sont survenus

16. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

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

au moment des faits et qui auraient pu compromettre le fonctionnement de cette chaîne (une coupure de courant par exemple).

Par ailleurs, à supposer qu'elles puissent théoriquement aboutir, ces expertises sont extrêmement délicates, longues et complexes, ce qui les rend onéreuses et par conséquent disproportionnées au regard du montant des litiges, eu égard à la matière. Les parties n'auront donc pas intérêt, économiquement, à introduire une action en justice aux fins de solliciter une expertise coûteuse au regard du gain espéré.

Puisqu'une résolution a posteriori des difficultés paraît peu opportune, il serait bien plus pertinent de réfléchir à des solutions permettant d'éviter sinon de contourner le problème.

4.2.2 La nécessaire prévention des difficultés

L'informatique est une science jeune. Les méthodes de développement de programmes ont considérablement évolué avec la mise au point de règles d'écriture, de campagnes de tests, etc. Pourtant des bugs subsistent et ne sauraient complètement disparaître (du fait, notamment de l'existence de bugs d'exécution). Une nouvelle étape pourrait être la prise en compte de l'existence de bugs, même s'ils ne sont pas identifiés, dès l'étape du développement, en dotant les usagers de la capacité de signaler des dysfonctionnements dès leur constat. Il serait également nécessaire de disposer de méthodologie permettant d'identifier les systèmes numériques qui sont des SIN pour, ensuite, envisager leur amélioration.

Ainsi, pour prévenir ces difficultés probatoires liées à l'usage des systèmes inéquitables numériques, est-il envisageable de renverser la charge de la preuve ? En principe, si l'usage du système inéquitable matérialise l'exécution d'une obligation civile, ce devrait être à l'usager débiteur de cette obligation de prouver qu'il s'est correctement exécuté. Or, puisque la preuve est détenue par le prestataire de services, il serait sans doute envisageable de renverser la charge de la preuve pour qu'elle pèse sur celui-ci.

Cette solution ne fait toutefois que déplacer le problème : le prestataire démontrera, à l'aide des traces dont il dispose, que l'utilisateur n'a pas correctement exécuté son obligation, ce qui n'empêchera pas l'usager de contester ce fait en soutenant qu'il y a eu un bug dans le système et donc en demandant une expertise.

La solution la plus pertinente serait donc de permettre à l'usager de détenir *a priori* des éléments pour prouver sa bonne foi. En d'autres termes, il faut rétablir la symétrie de l'accès à la preuve. Cette solution est d'ailleurs déjà mise en œuvre dans le cadre de certains systèmes identifiés plus haut comme pouvant être des systèmes inéquitables numériques. Ainsi, à Paris, il est possible de retirer un ticket aux bornes Vélib pour attester que le vélo a été correctement reposé, étant précisé que cette solution n'est pas infaillible non plus puisque des problèmes de panne d'imprimante, d'absence de papier ou d'encre peuvent subvenir. A l'Université de Nantes, les étudiants déposant un devoir ou réalisant un test noté sur une plate-forme dédiée peuvent maintenant obtenir un accusé de réception qu'ils peuvent conserver.

Une autre possibilité équivalente mais relevant du domaine du numérique serait d'envisager l'envoi d'un message électronique ou d'un SMS ou encore la production d'un fichier signé téléchargeable (par exemple en s'inspirant des preuves d'envoi de

Lettres recommandées en ligne par La Poste) que l'utilisateur pourrait conserver. Toutefois, quand elle est réalisée, cette procédure doit être étudiée avec précision afin d'éviter certains écueils. Ainsi, l'envoi d'un simple message électronique est insuffisant car il n'existe pas de garantie de délivrance des courriers électroniques : un message électronique peut ne jamais parvenir à son destinataire ou ne lui parvenir qu'après des semaines de délai.

Cette approche reste cependant prometteuse et devrait être approfondie car elle a pour conséquence d'éliminer *in fine* les SIN.

5 Nouvelle conclusion

Malgré la confiance aveugle qui est accordée aux systèmes numériques, il est nécessaire aujourd'hui d'admettre qu'ils dysfonctionnent parfois. Cette première observation se heurte toutefois à l'idée reçue par nombre de personnes non informaticiennes selon laquelle les systèmes numériques sont quasiment infaillibles. Différentes mesures peuvent être déployées pour que des utilisateurs confrontés à des dysfonctionnements numériques ne soient pas, *en sus*, accusés de diverses infractions comme la fraude ou le vol.

Éduquer les magistrats et avocats quant au fonctionnement et aux fragilités des programmes informatiques serait certainement souhaitable. Mais une double formation, à la fois au droit et à l'informatique, nécessiterait des doubles cursus et donc un allongement des études ou une densification des enseignements, ce qui paraît difficilement généralisable. De plus, les juristes déjà en activité ne bénéficieraient pas de ces nouveaux savoirs. Cette voie ne semble donc pas praticable. En revanche il serait possible de doter les logiciels de nouvelles fonctionnalités permettant d'appréhender l'étendue des dysfonctionnements : effectuer des mesures quantitatives des pannes, donner la possibilité aux utilisateurs de signaler des dysfonctionnements. L'existence même de ces fonctionnalités tendrait à modifier l'a priori du grand public (et donc des juristes) quant à la perfection des systèmes numériques. La mise en œuvre de telles disposition doit être initiée dès la conception des systèmes numériques. Cette démarche nécessite donc une nouvelle approche intellectuelle : il s'agit, en amont, d'imaginer différents scénarios de panne et d'estimer dans quelle mesure les utilisateurs peuvent en être les victimes.

Les systèmes numériques qui existent déjà et qui ne sont pas dotés de telles capacités, devraient pouvoir être identifiés et, pourquoi pas ?, classés en fonction des risques encourus par les utilisateurs et du caractère obligatoire ou optionnel de leur usage. En effet, s'il est possible de se priver d'une bicyclette en libre-service, il est plus difficile de renoncer aux droits sociaux ou aux services de pôle emploi pour lesquels les interactions avec des dispositifs numériques sont imposés. Il apparaît donc nécessaire de développer une grille d'analyse des systèmes informatiques existants afin de révéler les risques encourus par les utilisateurs pour, éventuellement, tenter d'y remédier par des corrections informatiques.

Nous avons bien conscience que ces réflexions s'inscrivent dans une réflexion éthique (il s'agit de protéger l'utilisateur qui est la partie juridiquement faible) qui peut sembler

contradictoire avec le discours promotionnel et mélioratif qui accompagne actuellement le développement du numérique. Toutefois, les utilisateurs, maintenant nombreux avec la généralisation des ordiphones, accumulent des expériences : le temps passant, les constats de dysfonctionnements du numérique deviennent courants. Cette meilleure perception des fragilités du numérique peut engendrer une moindre acceptabilité des discours promotionnels. *A contrario*, les utilisateurs pourraient d'autant plus apprécier des dispositifs qui prennent en compte leur expérience réelle et leurs intérêts. Ces qualités éthiques pourraient être mises en avant et devenir de nouveaux arguments promotionnels.

Bibliographie

[1] Bergeaud-Wetterwald, A. Le droit à la preuve, préf. J.-C. Saint-Pau, LGDJ, 2010, Coll. Bib. Dr. privé, spéc. n° 329.

[2] Cadiet, L. Normand, J. Amrani-Mekki, S. Théorie générale du procès, 2e édition, PUF, 2013, Coll. Thémis Droit, n°21.

[3] Gorman, O. The Effect of Cosmic Rays on the Soft Error Rate of a DRAM at Ground Level, IEEE Transactions on Electron Devices, vol.41, issue 4, p.553-557, (April 1994).

[4] Migayron, S. Critères d'appréciation techniques, vraies et fausses preuves numériques. intervention à l'occasion du colloque du 13 avril 2010 à la première chambre de la Cour d'appel de Paris, consacré à « La preuve numérique à l'épreuve du litige » - Consulté le 8 décembre 2017.

[5] VLS France JCDecaux. Rapport du Médiateur 2014.