Les tribunaux à l'ère du numérique et ... des législations de protection des données

Poullet, Yves

Published in:
Le tribunal de l'Union européenne à l'ère du numérique

Publication date:
2019

Document Version
le PDF de l'éditeur

Yves Poullet
Professeur à l'université de Namur et de Lille
(Belgique et France)

Intervention de M. Yves Poullet, Professeur à l'université de Namur et de Lille (Belgique et France)

Les tribunaux à l'heure du numérique et… des législations de protection des données : de quelques zones d'incertitude

1. Le numérique, un apport incontestable à la Justice – Nul ne songe à remettre en cause l'apport considérable des outils modernes de gestion de l'information et de la communication au travail des magistrats et des parquets. Pour le parquet, la contribution du numérique à l'élucidation des affaires est évidente : plus de 70 % des crimes trouvent dans les traces laissées par leurs auteurs la solution et le numérique facilite la recherche des suspects voire la découverte de l'auteur. Les lois de procédure criminelle ont ainsi largement légitimé l'usage des outils du numérique. Pour la magistrature, l'apport peut se caractériser de diverses façons : le premier est certes leur contribution à une meilleure efficacité des procédures judiciaires, et ce depuis l'accès au tribunal jusqu'à la communication du jugement final et à son exécution. Il s'agit par là même de rendre un meilleur service au justiciable par une accélération de la procédure, un meilleur accès aux pièces et une communication facilitée [1]. Le second apport touche à la qualité du contenu du jugement. Le numérique permet un traitement des affaires plus approfondi par une meilleure accessibilité aux éléments du dossier et au-delà aux précédents judiciaires non seulement identifiés, mais, grâce aux systèmes d'intelligence artificielle, analysés et comparés. Les mêmes systèmes peuvent aider à la rédaction de la sentence voire à sa rédaction elle-même, pour autant qu'on cède au mythe d'un « juge-robot » qui vous remplacerait, au dire de certains, plus efficacement et de manière plus objective [2], Mesdames et Messieurs les juges.

Soyons clair, loin de nous l'idée de nous opposer à l'utilisation de l'outil d'efficacité et de meilleur service aux justiciables que représentent les technologies de l'information et de la communication et d'appeler les greffiers, juges et auxiliaires de la justice à conserver leur culture papier. Nous pensons au contraire qu'il y a danger pour les tribunaux à ne pas s'adapter à de

1| Sur tous ces avantages et une analyse comparée des avancées en la matière, lire E-Justice, *Using Information Communication Technologies in the Court System*, A. Cerillo et P. Fabra (eds), Information Science Reference, 20, Hershey, 2010.

2| A. VAN DEN BRANDEN (*Les robots à l'assaut de la Justice*, Larcier, 2018) compare ainsi systématiquement l'office du juge-robot à celui du juge humain sur bien des critères et proclame *in fine* la victoire du premier sur le second.

telles technologies : danger de voir demain les citoyens se tourner vers des justices privées dont on vantera l'efficacité ; danger de ne plus être en mesure de pouvoir discuter à égalité avec certains professionnels, assénant leur soi-disant vérité, parce que sortie des ordinateurs. S'il faut résolument faire entrer le monde judiciaire dans l'ère de l'Internet, il est cependant important que les décisions soient prises après réflexion et avec sa pleine participation et que l'apport des technologies nouvelles soit pleinement respectueux de nos libertés et des principes mêmes qui constituent les exigences du *« fair trial »*.

2. Le propos de la contribution – Ces apports ont des limites. Notre contribution en pointe une source en particulier : les textes européens récents en matière de protection des données : le RGPD [3] et la directive 2016/680 [4] sur les traitements relatifs aux infractions pénales [5]. Notre propos entend analyser la façon dont ces deux législations amènent à des modifications du travail des juges et des parquets, voire à la création de nouveaux organes ou fonctions. Cette question a peu été abordée jusqu'à présent [6]. Or elle est à la fois essentielle et délicate. Essentielle dans la mesure où les impératifs d'efficience et d'optimisation qu'apporte l'utilisation des TIC n'ont de sens que si, parallèlement, les enjeux et principes fondamentaux régissant l'action judiciaire sont respectés. Parmi ces enjeux, et sans nier l'importance d'autres principes [7] que les applications numériques risquent de remettre en cause, celui des libertés fondamentales et en particulier de la protection des données doit être pris en considération. Par ailleurs, la numérisation du fonctionnement de nos tribunaux accélère le mouvement de transformation d'un pouvoir à l'agir « opaque » en une organisation au sein de laquelle les flux sont encadrés et réglementés. Sans doute nos codes de procédure civile et criminelle constituaient déjà un

3| 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).

4| Directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

5| Sur cette directive, voir notamment l'analyse de C. FORGET, « La protection des données dans le secteur de la police et de la justice », in *Le règlement général sur la protection des données, analyse approfondie*, de Terwangne et Rosier (eds), Cahier du CRIDS, n° 44, 2018, p. 865 et suivantes.

6| Voir cependant, en Belgique, le remarquable article de F. DANIELI, « L'application de la loi vie privée au pouvoir judiciaire et au secteur policier : disaster... or much about nothing ? », RDTI, 2007, p. 169 et suivantes ; cf. également Y. Poullet et D. Moreau, « La justice au risque de la vie privée », in *Phenix et la procédure électronique*, op. cit., p. 87 et suivantes, et H. Van Bossuyt, « Het informatiesysteem Phenix : een nieuw hulpmiddel voor justitie », R.A.B.G., 2005, p. 1435 et suivantes.

7| Nous reviendrons sur ce point en conclusion de la contribution.

cadre à ce fonctionnement, mais il est clair que les réglementations de protection des données ont bien cet objectif et obligent, comme on le notera, à souvent mieux préciser ce cadre.

I. Applicabilité des textes au pouvoir judiciaire et aux parquets

3. Deux questions préjudicielles – Sans doute nous faut-il répondre aux deux questions préjudicielles suivantes : le RGPD et la directive sont-ils applicables à nos tribunaux ? Et, en cas de réponse positive : à quelle réglementation (Règlement ou Directive) les traitements mis en œuvre par nos parquets et nos juges doivent-ils répondre ? Si, sur le premier point, hormis une nuance importante, la réponse est positive, sur le second point, la réponse est plus difficile.

4. L'applicabilité des textes – À cette première question, on note la réponse identique apportée tant par le considérant n° 20 du RGPD que celui n° 80 de la Directive : *« Bien que le présent règlement s'applique, entre autres, aux activités des juridictions et autres autorités judiciaires, le droit de l'Union ou le droit des États membres pourrait préciser les opérations et procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et autres autorités judiciaires.* ***La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle*** [8]***,*** *afin de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions. Il devrait être possible de confier le contrôle de ces opérations de traitement de données à des organes spécifiques au sein de l'appareil judiciaire de l'État membre, qui devraient notamment garantir le respect des règles du présent règlement, sensibiliser davantage les membres du pouvoir judiciaire aux obligations qui leur incombent en vertu du présent règlement et traiter les réclamations concernant ces opérations de traitement de données. »* En d'autres termes, se dégagent de ces considérants trois principes : le premier est l'application des textes aux juridictions de l'ordre judiciaire et aux autres autorités juridictionnelles [9]. Le deuxième nuance cependant cette application. Eu égard à l'indépendance du pouvoir judiciaire, la compétence des APD ne s'étend pas ***« au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle »***. Troisièmement, le contrôle des textes doit pour ces traitements être exercé par une autorité spécifique au sein de l'appareil judiciaire. Cette prise de position n'est pas sans soulever des questions quant aux traitements couverts par l'exception. Que

8| Nous soulignons.

9| Ainsi, l'ensemble des juridictions administratives, mais également des commissions ayant dans des domaines donnés une compétence pour trancher les litiges.

signifie « dans l'exercice de leur fonction juridictionnelle » ? *A priori*, des pans entiers de l'activité de nos tribunaux semblent ne pas devoir être couverts par l'exception : ainsi, la constitution d'une base de données des jugements, les activités administratives des greffes, les enquêtes des parquets, etc. Par ailleurs, les activités des juges d'instruction, à l'inverse de celles du ministère public, rentreraient dans l'exception. Il y a donc risque d'interventions de diverses autorités de contrôle au sein de la même organisation du tribunal, et ce pour que des traitements soient partagés. Par exemple, peut-on imaginer des autorités différentes entre le parquet et le juge d'instruction, alors que leurs traitements relèvent bien souvent de la continuité d'une opération ou d'une affaire ? Enfin, mais nous reviendrons là-dessus (*infra*, n° 28), quelle autorité de contrôle mettre en place « au sein » du pouvoir judiciaire, mais en même temps suffisamment indépendante de son autorité ?

5. Applicabilité, oui, mais de quel texte ? Une seconde question est la délimitation difficile des champs d'application des deux textes, dont les dispositions diffèrent et pour lesquels la marge de manœuvre des États n'est pas la même. Au-delà, on souligne que nombre de principes du RGPD se retrouvent avec bien des nuances dans la Directive. La Directive a en effet tenu compte déjà d'un certain nombre de dérogations, nécessaires à l'intérêt général et bien compréhensibles en matière de prévention et de lutte contre les infractions pénales, comme il sera montré plus loin. Bref, suivant que l'on se trouve dans le champ d'application de l'un ou l'autre texte, les solutions varieront. On souligne ainsi que la directive 216/680 s'applique aux traitements des parquets mais non des juges, qui seraient, même en matière pénale, soumis au RGPD. Par contre, la notion d'« infraction pénale », étant définie largement par la CJUE [10] comme toute infraction à la loi donnant lieu à une sanction recouvrant un « caractère punitif et dissuasif », conduit à l'application de la Directive à des services, y compris privés, chargés de l'inspection ou du contrôle de lois pénales comme le blanchiment d'argent, mais également aux juridictions ou commissions d'enquêtes s'occupant d'infractions aux lois fiscales, sociales, aux droits de la concurrence, de la consommation, de la protection des données. Enfin, on s'interrogera sur la difficulté de déterminer le texte applicable en cas de transmission volontaire ou forcée par une entreprise soumise au RGPD aux services de police judiciaire ou non dans le cadre d'une enquête à propos d'une infraction pénale.

10| Le considérant n° 13 rappelle ainsi la jurisprudence de la CJUE, en particulier l'arrêt du 27 mai 2014, Spasic, C-129/14 PPU, EU:C:2014:586.

II. Le contenu des textes applicables aux juridictions et parquets

6. Réflexions liminaires – Mais ces questions « préjudicielles » pointées, venons-en au contenu des législations de protection des données. Certes, la plupart des exigences sont prises en compte par les législations de procédure civile ou pénale déjà actuellement en vigueur (exemple : le jugement est motivé, la personne concernée a accès à son dossier, y compris pénal, ...), cependant **certaines exigences des législations de protection des données réclament des adaptations de la pratique et/ou la création de nouveaux organes**. En outre, les textes autorisent des marges de manœuvre aux États européens qui peuvent se révéler dommageables pour la création d'un espace judiciaire européen [11]. La suite de notre exposé entend relever ces conséquences et risques suivant le plan qu'imposent les réglementations de protection des données. Pour aborder ces différents points, nous suivrons le plan proposé par les réglementations de protection des données, à savoir : le point A s'attachera à quelques définitions dont la portée mérite quelques explications, confrontées à la réalité de la conception et de la mise en œuvre des traitements dans l'ordre judiciaire. Au point B, seront examinés les principes de base des traitements, principes communs aux deux réglementations, mais dont la signification n'est pas nécessairement la même suivant les deux textes. Les droits de la personne concernée surtout dans le cadre des procédures pénales feront l'objet du point C. Le point D s'attardera en particulier sur deux obligations complémentaires du responsable, voire du sous-traitant. Enfin, on évoquera (point E) la question délicate déjà évoquée de l'autorité de contrôle.

A. Les définitions

7. Donnée anonyme – Les législations de protection des données ne s'appliquent **pas aux données anonymes**. L'anonymat lors de la publication des jugements est dans tous nos pays un débat délicat (voir par exemple le rapport CADIET [12] en France) qui renvoie à de nombreuses questions. S'agit-il d'anonymisation, de pseudonymisation ou d'occultation, terme choisi par le

11| Un exemple parmi d'autres est la diversité des solutions trouvées dans les différents pays à la question de l'anonymisation des jugements.

12| Sur tout le débat en France, lire B. MATTHIS et H. RUGGIERI, « L'open data des décisions de justice en France », in Actes du colloque du 8 juin 2018 organisé par le CRIDS de l'université de Namur : « Le juge et l'algorithme : Juges augmentés ou Justice diminuée ? », Cahier du CRIDS, n° 46, 2019, p.197 et s.

récent décret français [13] ? L'anonymisation est-elle assurée d'office ou à la demande ? Comment, si anonymisation il y a, résoudre le problème du chaînage des décisions et la nécessité de conserver au sein de la justice une base de données non anonymisée ? Jusqu'où (par exemple, quid de la mention d'un compte bancaire ?) et à propos de qui (parties au procès, autres personnes citées par le jugement, avocats, magistrats) ? Comment y procéder ? [14]

8. Donnée judiciaire – La **« donnée judiciaire »** est une donnée sensible, elle est définie par l'article 10 du RGPD, qui reprend sans la modifier la définition de l'article 8 de la directive 95/47 : *« Le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes fondé sur l'article 6, paragraphe 1, ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.' »* Ces restrictions sévères visent à éviter la double peine : celle qui résulte du prononcé de la sanction par le juge et celle qui s'ajouterait du fait de l'opprobre qui fait suite à la publication par les journaux, relayée ensuite par les sites web et les moteurs de recherche. On ajoute que là où le droit connaît le « pardon » de la prescription, la mémoire de l'ordinateur n'a pas de limite temporelle. Sans doute ces éditeurs et ces moteurs de recherche se réclament-ils de la liberté d'expression pour justifier la mise à disposition du public non du jugement mais d'un commentaire de celui-ci. On connaît la solution dégagée par le RGPD, ouvrant le droit de la personne concernée au « déférencement » [15]. L'article 1 de la Directive envisage de manière centrale – c'est l'objet même de la Directive – les données traitées *« 'par les autorités* ***compétentes*** [16] *à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »*. Ces données font l'objet de sévères limites et, en principe, ne peuvent être utilisées que pour les

13| Selon les termes de l'article 19 du projet de loi française de programmation et de réforme de la justice 2018- 2024 : « *"Occulter" veut dire effacer, tandis que "pseudonymiser" signifie remplacer un nom par un autre* » (MATTIS – RUGGIERI).

14| Sur tous ces points, lire B. MATHIS et H. RUGGIERI, « L'*open data* des décisions de justice en France – . Les enjeux de la mise en œuvre », in Justice et Algorihme, Cahier du CRIDS, n° 46, 2019, p. 195 et suivantes ; B. DOCQUIR, « Quelques observations complémentaires sur la publication des décisions », *J. T.,* 2019, p. 449 et suivantes.

15| Arrêt du 13 mai 2014, Google Spain et Google, C-131/12, EU:C:2014:317. Pour un commentaire, lire Q. VAN ENIS, « Le droit de recevoir des informations ou des idées par le biais d'Internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *JEDH,* 2015/2, p. 178 et suivantes.

16| Attention, une entreprise privée (par exemple la banque dans le cadre de ses obligations légales fondées sur la lutte contre le blanchiment d'argent peut traiter des « données judiciaires » au sens du RGPD, de même une entreprise peut noter des suspicions de fraude de la part de ses employés voir de tiers relatifs à des opérations de l'entreprise.

finalités énoncées par la loi et soumises à des conditions sévères, et on peut en inférer que l'utilisation de telles données en dehors de telles finalités est interdite.

9. Responsable du traitement et sous-traitant – Le **« responsable du traitement »**, auquel nombre d'obligations sont attachées, est défini tant par le RGPD que la Directive comme celui *« qui, seul ou conjointement, définit les finalités et les moyens »*. Cette définition soulève les questions suivantes : la première souligne que le choix des moyens informatiques de la justice et le choix des sous-traitants sont rarement le fait de la Justice mais, bien plus souvent, celui de l'administration, voire résultent de la collaboration du palais avec les barreaux [17]. Faut-il alors parler de responsabilité « conjointe » entre l'administration voire les barreaux, d'une part, et le pouvoir judiciaire, d'autre part ? Si oui, quelle répartition des tâches ? Ne faut-il pas créer au sein du pouvoir judiciaire un organe qui puisse intervenir avec expertise dans la définition des moyens électroniques mis en place ? Seconde question : l'organisation judiciaire est-elle une ou plurielle? Faut-il prévoir différents responsables de traitement, en arguant que les traitements suivant le degré ou la nature de la juridiction ont des caractéristiques différentes ? Ainsi, on pourrait distinguer le niveau central et les niveaux décentralisés, voire au niveau de chaque dossier (le magistrat en charge du dossier).

On conçoit aisément les difficultés qu'entraînerait une telle multiplication des responsables. Parmi les définitions, on souligne celle de sous-traitant : *« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».* La multiplication des appels à des sous-traitants (sociétés de consultants, firmes de logiciels) pour la numérisation des opérations des tribunaux voire l'outsourcing de certaines fonctions constituent un risque important de perte de maîtrise par le pouvoir judiciaire de la conception des systèmes qui lui sont fournis ou qui sont gérés en dehors de lui. Il est important que, conformément aux textes de protection des données, le pouvoir judiciaire en tant que responsable définisse contractuellement la mission et les obligations du sous-traitant, en particulier celles de sécurité.

17| Ainsi, l'application « e-Deposit » (dépôts électroniques de conclusions) a été développée en Belgique à l'initiative des barreaux d'avocats. Toujours en Belgique, on citera le passage suivant du plan « e-justice » du ministre de la Justice actuel : *« Les prestataires de services judiciaires, comme les avocats, les huissiers de justice, les notaires et les experts, seront activement impliqués dans le développement d'un certain nombre de projets d'informatisation et dans la réalisation de l'indispensable changement de culture. En 2015 et 2016, on misera fortement sur une collaboration active des professions juridiques et des prestataires de services dans le cadre de l'informatisation de la Justice. La plupart d'entre eux sont, depuis plusieurs années déjà, actifs sur les autoroutes électroniques de l'information et sont déjà plus avancés dans le changement de culture et le développement de systèmes informatiques. Ils ont également participé auparavant au succès enregistré dans un certain nombre de projets d'informatisation (exécution de la loi Salduz, banques de données des avis de saisie, registre central des testaments…). »*

Nous mentionnons enfin la notion de destinataire, définie de manière semblable par l'article 4.9 du RGPD et l'article 3.10 de la Directive: *« la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers »*. La Directive ajoute cependant : ***« Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière [...]... ne sont pas considérées comme des destinataires. »*** On devine l'intérêt de cette définition large, qui contredit pourtant la définition de « destinataire ». Elle facilite les communications et flux d'informations entre entités, y compris distinctes, dans le cadre de la lutte contre les infractions pénales, sans que les obligations d'information des personnes concernées ne limitent ces flux.

B. Les principes applicables à tout traitement

10. Le principe de finalité – Passons aux principes de la protection des données. Ils sont nombreux, mais le premier est sans doute essentiel : tout traitement doit poursuivre **des finalités déterminées, explicites et légitimes et ne pas utiliser les données à caractère perronnel de manière incompatible avec ces finalités**. C'est en tout cas l'énoncé du principe tel qu'il figure à l'article 5 du RGPD. Nous verrons combien la Directive le nuance. Pour revenir au principe, la loi belge du 10 août 2005 instituant le système d'information Phénix [18] confiait au système d'information Phénix, qui couvrait l'ensemble des fonctions de l'organisation judiciaire, les finalités suivantes [19] :

- Communication interne (au sein de l'organisation judiciaire) et externe (avec les parties) aux fins d'initier la procédure, d'échanger les points de vue et de traiter, sur le fond et la forme, le litige.
- Communication externe aux fins de faire exécuter la décision.
- Gestion et conservation des données judiciaires.

18| M. b., 19 sept. 2005. Cette loi a été modifiée depuis à plusieurs reprises, mais sans modification de la liste des finalités (sur ces modifications, lire D. MOUGENOT – Y. POULLET, « Le Phénix renaîtra-t-il de ses cendres », in *E-Justice 2020, Les enjeux du futur*, SPF Justice, Maklu, 2018, p. 77 et suivantes.

19| La loi du 8 décembre 1992 sur la protection des données à caractère personnel interprétée à la lumière de l'arrêt de la Cour EDH du 4 mai 2000, Rotaru c. Roumanie (CE:ECHR:2000:0504JUD002834195), imposait en effet au législateur de définir les finalités des traitements de données mis en place. Sur ce point, lire : D. Moreau et Y. Poullet, « La justice au risque de la vie privée », in *Phénix et la procédure électronique*, CUP, Formation permanente, vol. 85, dir. J.-F. Henrotte, Larcier, 2006, p. 87 et suivantes ; F. Danieli, « L'application de la loi vie privée au pouvoir judiciaire et au secteur policier : disaster... or much about nothing ? », RDTI, 2007, p. 169 et suivantes.

- Création d'un rôle national qui attribue à chaque affaire un numéro qui permettra d'en assurer le suivi.
- Création et diffusion d'une base de données jurisprudentielles.
- Élaboration de statistiques aux fins d'amélioration du fonctionnement de la Justice.
- Gestion et administration des institutions judiciaires.

Pour revenir à un concept évoqué à l'entrée de la réflexion pour définir le régime dérogatoire du système judiciaire par rapport au régime général, il semble que seule la première finalité corresponde à ce que le RGPD appelait la finalité ***d'exercice de la fonction juridictionnelle*** proprement dite. Cette division couplée avec le principe de finalité plaide pour une certaine séparation des différents traitements relevant de ces diverses finalités. L'article 6.4 du RGPD permet cependant l'utilisation à d'autres fins qu'initiales à condition que ces nouvelles finalités soient compatibles. Cinq critères sont énoncés pour juger de la compatibilité : le lien entre les finalités envisagées, le contexte, la nature des données, les conséquences du nouveau traitement et, enfin, les garanties apportées en particulier en matière de sécurité.

11. Directive et principe de finalité – Pour la directive 2016/680, les finalités couvrent à la fois la prévention (par exemple l'utilisation par le parquet d'un système d'IA permettant de repérer des auteurs potentiels de futures infractions ou le logiciel COMPAS utilisé aux EU pour mesurer les risques de récidive) et la détection d'infractions de même que le suivi de l'exécution des peines [20]. L'article 4.2 ajoute que *« le traitement, par le même ou par un autre responsable du traitement, pour l'une des finalités énoncées à l'article 1er, paragraphe 1, autre que celles pour lesquelles les données ont été collectées, est autorisé ».* Certes, deux conditions sont ajoutées, mais cette autorisation a pour conséquence de permettre le transfert facile de données entre responsables (par exemple la police et le parquet) selon une conception holistique des traitements intervenant dans une même enquête voire dans des enquêtes différentes au nom de la connexion possible des affaires, et ce peu importe la dualité de responsables : ainsi, le principe de compatibilité serait respecté si, au cours de l'instruction, la police découvrait des faits susceptibles d'une autre incrimination dont le parquet a la charge et transmettait à ce dernier les éléments de l'enquête pour faciliter l'enquête. L'autorisation permettrait également, à la limite – la réponse positive est ici plus discutable – , le transfert

20| Sur l'utilisation des données dans le cadre des procédures policières, lire J. W. HOLLAND, « Digital Government and Criminal Justice », in E-Justice, *Using Information Communication Technologies in the Court System*, A. Cerillo et P. Fabra (eds), Information Science Reference, 20, Hershey, 2010, p. 152 et suivantes.

de données entre des traitements créés dans le cadre, d'une part, de la lutte antiterroriste et, d'autre part, de la lutte contre l'immigration clandestine.

Enfin, dernière question : quid de la transmission volontaire ou non de données d'entreprises privées à la police ou au parquet, ainsi la communication d'images vidéo prises par un grand magasin aux fins de retrouver une personne disparue ou le transfert des données de *surfing* conservées par une plateforme pour retrouver l'auteur de messages racistes ? Faut-il appliquer le RGPD, ce qui rendrait difficile le transfert vu l'incompatibilité des finalités, ou faut-il appliquer la Directive, ce qui rendrait plus facile la transmission, au nom de l'absorption du traitement privé dans celui visé par la Directive, comme le défend la thèse récente de C. Jasserand [21] ?

12. Le second principe exige la loyauté et la licéité du traitement – L'article 8.1 de la Directive énonce : *« Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1… […] »* Soit, mais, en matière pénale, le considérant n°27 semble affirmer le principe de la compatibilité *a priori* des données collectées à la finalité. Autre point, plus délicat encore : la question de la prise en compte dans les traitements et dès lors dans les décisions de données obtenues illicitement (ainsi, par exemple, les images obtenues par une caméra de vidéosurveillance non autorisée pour justifier le licenciement d'un travailleur). Le traitement de telles données devrait être jugé illicite, sauf à considérer – mais la loi [au sens très large de la Convention du Conseil de l'Europe (voir considérant nº 32 de la Directive)] est alors nécessaire – que le juge peut en tenir compte. L'exemple belge est intéressant à citer : la jurisprudence belge, développée à partir de l'arrêt dit « Antigone » [22], a progressivement admis de manière répétée [23] qu'un moyen de preuve même acquis illicitement ne devait pas être écarté sur la seule base de son illicéité, lorsque les faits ainsi établis sont d'une gravité telle que l'illicéité du moyen de preuve peut être écartée et moyennant quelques conditions supplémentaires. Cette jurisprudence, dans la mesure où elle est bien établie et largement connue et reconnue, peut être considérée comme une loi au sens que l'interprétation de la Cour de Strasbourg donne au terme loi. Il n'empêche que le législateur belge, pour écarter

21| C. JASSERAND, *Reprocessing of biometric data for law enforcement purposes*, Ph. D. thesis, Univ. of Groningen, 2019. Pour plus de détails sur les organes de Phenix, voy. Y. Poullet et D. Moreau, « La justice au risque de la vie privée », in *Phenix et la procédure électronique*, op. cit., p. 87 et suivantes ; H. Van Bossuyt, « Het informatiesysteem Phenix : een nieuw hulpmiddel voor justitie », R.A.B.G., 2005, p. 1435 et suivantes.

22| Cass. nº 86/2002, 8 mai 2002, B. S., 24 mai 2002.

23| À ce sujet, voir les références et la réflexion du Procureur général à la cour d'appel d'Anvers, Y. LIÉGEOIS, dans la mercuriale prononcée le 3 septembre 2007.

tout doute à ce sujet, a légiféré en la matière : l'article 32 du CIC belge édicte : *« La nullité d'un moyen de preuve obtenu irrégulièrement n'est décidée que si… »*

Dans le même sens, on s'interroge sur la question de l'équilibre à trouver entre les exigences de la protection des données et celles du principe de l'égalité des armes tirées de l'article 6, paragraphe 1, de la Convention du Conseil de l'Europe. Peut-on, comme l'ont décidé diverses hautes cours de justice, considérer que le fait au nom de la vie privée d'interdire à un justiciable de se prévaloir de certains éléments de preuve et le priver ainsi de toute chance de l'emporter soit contraire au principe du droit de chacun à un procès équitable [24] ?

13. Le troisième principe édicte la qualité des données, ce qui suppose la recherche de l'exactitude de leur contenu et leur mise à jour. C'est du moins ce que prescrit le RGPD. À propos de cette exigence, on note l'interprétation très large de la notion d'exactitude en matière de traitements d'infractions pénales : le considérant n° 30 de la Directive énonce en effet que : *« Dans le cadre des procédures judiciaires notamment, les déclarations contenant des données à caractère personnel sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables. Le principe d'exactitude ne devrait, par conséquent, pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une déclaration déterminée a été faite. »* On conçoit la raison de ce relatif laxisme en matière juridictionnelle : le but du traitement du litige est d'arriver à la « vérité judiciaire » telle qu'énoncée par le juge. L'exactitude des données ne peut donc être considérée comme un *a priori* ; à la limite, on peut en parler comme une fin, c'est-à-dire le résultat souhaité du jugement.

On ajoute que l'article 7 de cette même Directive oblige désormais les responsables de traitements (parquet et police) à vérifier les données avant transmission et à séparer clairement les données relatives à trois catégories de personnes et les données fondées sur des faits et celles sur des appréciations. À ce dernier propos, il serait sans doute utile de ranger dans cette seconde catégorie les personnes identifiées suite à l'application d'un système IA.

24| Cass. comm., 15 mai 2007, D. 2007, 2775, obs. A. LEPAPE. Sur cette question, M. SULYOCK : « In All Fairness… : A Comparative Analysis of the Past, Present and Future of Fair Trial Systems Outside of Europe », Attila Badó (ed.) : Fair Trial and Judicial Independence – Hungarian Perspectives, Springer, 2014, p. 101-141. Reprenons les conclusions de la thèse de cet auteur (*Protecting Privacy in a Fair Trial – Comparative Constitutional Analysis of Admissibility of Evidence obtained in Violation of Fundamental Rights*, Thèse, Szeged, Hongrie, 2017) : « *Albeit Thaman* [S. C. Thaman : Balancing Truth Against Human Rights : A Theory of Modern Exclusionary Rules, Stephen C. Thaman (ed.), Exclusionary Rules in Comparative Law, Springer, 2013] *argued this in terms of criminal procedure, through "mirror translation" (as migrating ideas) His conclusions are applicable to those aspects of civil procedure that we have covered in our research. "When balancing (i.e. the exercise of judicial discretion between competing interests) is allowed, it should […] not be undertaken by the trial judge, especially in those systems based on civil law, where the trial judge is simultaneously a trier of facts […]"– writes Thaman, and we agree.* »

14. La proportionnalité des données, c'est-à-dire la pertinence ou adéquation de leur traitement au regard de la finalité poursuivie, peut difficilement être appréciée *a priori :* c'est au juge de déterminer ce qui à ses yeux est pertinent et fondera son jugement. À cet égard, je déplore les recours menés par certains avocats devant les APD, estimant que telles ou telles données doivent être retirées des conclusions au motif qu'elles ne sont pas adéquates. C'est en effet préjuger du jugement des magistrats et risquer de nuire au droit à la défense, qui suppose que l'on puisse en justice faire feu de tout bois pour démontrer son bon droit ou l'absence de droits d'autrui.

15. La durée de conservation des données (à distinguer de l'archivage, qui implique que les données sont désormais séparées et soumises à des règles d'accès et d'utilisation différentes vu la finalité distincte de l'archivage) n'est pas facile. Le RGPD exige la proportionnalité de la conservation des données, mais, outre qu'il n'est pas clair que cette règle s'applique à la conservation des pièces, l'application de la règle risque d'être appréciée différemment au cas où ces données peuvent être utiles dans des affaires ultérieures, et certains affirmeront en ce sens le besoin d'une longue conservation des données.

La Directive autorise une conservation plus longue, mais, à nouveau, le texte manque de clarté sur l'ampleur de cet élargissement légal possible ! Le texte exige certes la fixation de délais maxima de conservation par le responsable [25] (ou le législateur) et la mise à jour des dossiers permettant le nettoyage régulier des données qui ne sont plus pertinentes. Au-delà, il est difficile de fixer des règles précises, dans la mesure où la conservation de données peut s'avérer utile dans le cadre de procédures bien ultérieures où il sera intéressant de retrouver ces dernières. Le considérant n° 27 de la Directive légitime d'ailleurs ces conservations longues de données dans le domaine de la lutte contre les infractions pénales et de leur prévention : *« Aux fins de la **prévention** des infractions pénales, et des enquêtes et poursuites en la matière, les autorités compétentes ont besoin de traiter des données à caractère personnel, collectées dans le cadre de la prévention et de la détection d'infractions pénales spécifiques, et des enquêtes et poursuites en la matière au-delà de ce cadre, pour acquérir une meilleure compréhension des activités criminelles et établir des liens entre les différentes infractions pénales mises au jour. »* D'autres questions méritent d'être posées : par exemple, la réhabilitation entraîne-t-elle suppression des données relatives à la personne réhabilitée ?

25| Sur ce point, on se référera au considérant no 26 : *« Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, **des délais devraient être fixés par le responsable du traitement en vue de leur effacement ou d'un examen périodique**. 'Les États membres devraient établir des garanties appropriées pour les données à caractère personnel conservées pendant des périodes plus longues à des fins archivistiques dans l'intérêt public, à des fins scientifiques, statistiques ou historiques. ».'*

16. On terminera avec le **principe de sécurité**, spécialement consacré par les textes nouveaux. Le principe est exprimé de manière identique dans le RGPD (article 32) et dans la Directive (article 29) : *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque , … […] »*

Les deux textes ajoutent une obligation de réévaluation périodique des mesures de sécurité. Le principe ainsi énoncé exige le contrôle des accès non seulement en interne mais également en externe, ainsi des auxiliaires de justice (avocats, huissiers) qui souhaitent utiliser les plateformes mises à leur disposition par la juridiction pour déposer des conclusions, fixer une audience, etc. Sans doute cette exigence conduit à l'octroi de moyens d'authentification électroniques à ces auxiliaires et, en ce qui concerne les traitements soumis à la Directive [26], la journalisation, c'est-à-dire la conservation systématique des logs d'accès en lecture ou en écriture et de communication. On s'interroge sur la conciliation de telles exigences avec le fait qu'il n'est pas rare qu'un avocat dûment mandaté se fasse représenter pour la défense de son client par un confrère du même cabinet, voire un confrère d'un autre cabinet. Dans ce cas, les contrôles ne pourront avoir lieu qu'*a posteriori*.

On ajoute, tant pour les responsables que pour les sous-traitants, l'obligation de notification de l'événement à l'autorité de contrôle, voire la communication de sa survenance aux personnes concernées en cas de brèches de sécurité. Ainsi, il apparaît que les textes de protection des données requièrent une attention sinon nouvelle, en tout cas renforcée, à la sécurité des traitements et des données.

26| Cf. l'article 25 de la Directive : *« 1. Les États membres prévoient que des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel. 2. Les journaux sont utilisés uniquement à des fins de vérification de la licéité du traitement, d'autocontrôle, de garantie de l'intégrité et de la sécurité des données à caractère personnel et à des fins de procédures pénales.* » Le Groupe de l'article 29, dans son avis de 2016 à propos de la Directive, estime que la journalisation est un *« outil crucial »* de la protection mise en place par la Directive.

C. Les droits de la personne concernée

17. Les codes de procédure civile et criminelle et les droits de la personne concernée : une traduction suffisante ? – Les **multiples droits de la personne concernée** consacrés par les réglementations européennes trouvent déjà dans les codes de procédure civile et criminelle une traduction adéquate en ce qui concerne l'accès, l'information et la correction. Ainsi, les modes introductifs d'instance, le jugement tiennent les mentions qui correspondent aux exigences des articles 13 et 14 du RGPD. Le droit d'accès est largement pris en compte par le caractère contradictoire de la procédure, y compris l'accès réciproque aux conclusions et le droit tant dans les procédures civiles que pénales de se faire remettre au greffe une copie certifiée conforme des pièces. Le principe même du contradictoire ouvre à chaque partie le droit de donner sa propre vision, mais également de « rectifier » l'opinion d'autrui. Le principe exige que, dans le cadre d'une procédure civile, des mémoires ou pièces communiqués avec retard soient écartés d'office des débats. Notre propos sera donc de relever les quelques points de divergence ou les exigences de complément que révèlent les dispositions du RGPD et surtout de la Directive.

18. L'information préalable – L'article 12 tant du RGPD que de la Directive prévoit une obligation du responsable de transparence sur les caractéristiques des traitements qu'il mène. On se plaît à souligner que nombre de juridictions en Europe ont créé des pages web reprenant les diverses informations exigées par les textes de protection des données, et ce « de façon concise, transparente, compréhensible et aisément accessible ». On cite ainsi les sites du Bundesverfassungsgerichtshof, ceux des Irish Courts et, plus récemment, d'Eurojust.

19. L'obligation d'informer en cas de collecte directe ou indirecte de données (article 13 du RGPD et article 13 de la Directive) – Cette exigence est largement prise en compte par nos codes de procédure. On souligne que l'article 14 de la Directive limite les informations à délivrer. L'article 13, paragraphe 3, de la Directive énonce : *« Les États membres peuvent adopter des mesures législatives visant à **retarder ou limiter** la fourniture des informations à la personne concernée en application du paragraphe 2, ou à ne pas fournir ces informations, dès lors et aussi longtemps qu'une mesure de cette nature constitue une mesure nécessaire et proportionnée dans une société démocratique, [...] pour ... : a) éviter de gêner des enquêtes, des recherches ou des procédures officielles ou judiciaires ; b) éviter de nuire à la prévention ou à la détection d'infractions pénales ... [...] »* Ces limitations répondent légitimement aux nécessités de pouvoir mener l'enquête en toute discrétion, même si ce devoir ne dispense pas les autorités judiciaires de leur obligation de *« traiter de façon correcte et consciencieuse les victimes d'infractions et leurs proches, en particulier en leur fournissant l'information nécessaire »* (article 3 bis du Code belge d'instruction criminelle).

20. Le droit d'accès — L'article 15 du RGPD est, nous l'avons dit, largement respecté par les exigences de nos codes de procédure civile relatives à la communication des conclusions dès le dépôt au greffe et le droit à la copie des pièces. L'article 15 de la Directive permet aux États membres de limiter le droit d'accès [27] : l'accès ne porte pas sur les données elles-mêmes ni *a fortiori* sur le résultat de leur traitement mais sur les catégories de données, les finalités du traitement, l'existence d'un droit à la rectification et à l'effacement et, enfin, les destinataires. Sur ce dernier point, on se souviendra de la définition restrictive donnée par la Directive de cette notion, qui limite fortement l'information à communiquer.

La Directive rappelle le droit de la personne concernée d'avoir copie de sa déclaration lors des phases d'information et d'instruction. Enfin, on sait que, dans nombre d'États membres, le Code de procédure pénale prévoit que, par exception au principe du secret de la procédure d'information et d'instruction justifié tant par le besoin d'efficacité de l'enquête que par le respect de la présomption d'innocence, le ministère public peut de manière discrétionnaire à la demande d'une partie lever le secret discrétionnaire [28]. En cas de refus par le ministère public, dont la Directive prend soin de préciser que la décision doit être écrite et motivée, la Directive crée un nouveau droit de la personne concernée, celui de demander l'accès via l'autorité de contrôle. En ce cas, est créé un droit d'accès indirect : l'autorité procédera à l'accès et, le cas échéant, demandera la rectification ou l'effacement réclamé, sans informer la personne concernée du résultat de l'exercice de l'accès si ce n'est le fait qu'elle y a procédé. Il est clair que ce droit conféré à l'autorité de contrôle va interférer avec la procédure actuelle et que le risque existe que le résultat de l'intervention de l'autorité de contrôle n'aboutisse à déjuger le ministère public. Enfin, la Directive soutient l'évolution de la plupart de nos pays européens vers un droit d'accès plus large à certains moments de la procédure, ainsi lors d'une décision de détention préventive et de la délivrance d'un mandat d'arrêt ou de comparution immédiate.

21. La rectification et l'effacement – Peu de choses à dire en ce qui concerne les procédures non pénales au sens large, dans la mesure où le principe du contradictoire est consacré par nos codes de procédure judiciaire ou administrative, qui prévoient le droit à la rectification et au complément, permis dans le cadre de l'échange des conclusions. Dans les procédures pénales au sens le plus large, on note la procédure de réouverture des débats et le droit du juge de corriger les erreurs matérielles ou de calcul.

27| L'article 15 énumère d'ailleurs les motifs de ces limitations : éviter de gêner l'enquête, éviter de nuire à la prévention et à la détection d'infractions pénales, protéger la sécurité publique, nationale ou les droits et libertés d'autrui …

28| « Cependant, Eurojust pourra refuser l'accès aux informations qui vous concernent, si nécessaire pour : lui permettre de remplir ses tâches et obligations ; protéger une enquête en cours au niveau national ; ou protéger les droits et libertés de tierces parties » (règlement « Protection des données » d'Eurojust publié en septembre 2019).

Certaines dispositions de la Directive limitent ces droits. L'article 17 de la Directive limite sévèrement le droit à l'effacement, l'article 16 écarte le principe du contradictoire pour les motifs déjà évoqués au stade de l'information et de l'instruction, le considérant n° 47 ajoute même que, *« en aucun cas, le droit de rectification ne pourrait affecter la teneur d'une déposition »,* même s'il reste à la personne le droit de réclamer une instruction ou une déclaration complémentaire. On ajoute que, si l'effacement est requis si les données sont inexactes et que le responsable doit communiquer cet effacement ou cette rectification aux services internes et externes. En cas de doute voire en cas de besoin de conservation à des fins probatoires, la Directive (article 17.3) lui permettra alors de préférer, à l'effacement, la limitation de l'utilisation des données « douteuses », par exemple en rendant les données inaccessibles ou en les transférant vers les services internes d'archivage. Dans un tel cas, il incombe au responsable d'informer du refus de l'effacement et de motiver celui-ci, sauf s'il peut se prévaloir (article 17.4) d'une législation satisfaisant aux exigences de la clarté, de la proportionnalité et considérée comme nécessaire dans une société démocratique (besoins de l'enquête ou intérêt général prépondérant).

22. Remarques finales à propos des droits de la personne concernée – Plus restreintes en ce qui concerne le RGPD, plus larges en ce qui concerne la Directive, dont le texte ouvre tant par le fait qu'il s'agit d'une Directive et que le libellé du texte lui-même de nombreux champs à des interventions législatives nationales, les possibilités accordées aux États membres de régler (jusqu'où ?) les droits de la personne concernée par des législations *ad hoc* (article 18) posent problème. Premier point à soulever : est-il possible d'atteindre une véritable uniformisation des pratiques des responsables, alors même que magistrats, polices et organismes de prévention et de répression de la criminalité sont appelés à coopérer ? Cette difficulté d'harmonisation, deuxième point, risque d'être plus grande encore si on n'accepte, comme certains pays s'apprêtent à le faire sans autre vérification, que la simple référence par les législations nationales de protection des données aux codes de procédure civile et d'instruction criminelle. Il est vrai que nos codes contiennent déjà la traduction adéquate de la plupart des dispositions de ces législations, mais encore faut-il le vérifier et sans doute réorganiser les textes de manière à mieux montrer comment ils traduisent les dispositions des textes européens de protection des données. Un troisième point a été souligné : l'autorité de contrôle reçoit dans le texte de la Directive une compétence d'intervention dans le cadre de l'exercice des droits de la personne concernée [29]. Cette possibilité d'interférence de l'autorité

29| *«1. Dans les cas visés à l'article 13, paragraphe 3, à l'article 15, paragraphe 3, et à l'article 16, paragraphe 4, les États membres adoptent des mesures afin que les droits de la personne concernée puissent également être exercés par l'intermédiaire de l'autorité de contrôle compétente... [...] 3. Lorsque le droit visé au paragraphe 1 est exercé, l'autorité de contrôle informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel. »*

de contrôle dans les décisions du ministère public se voit renforcée par la disposition générale de l'article 17, qui consacre un droit de recours à cette autorité de contrôle.

D. De quelques obligations complémentaires des responsables et sous-traitants

23. Quatre obligations du responsable (et des sous-traitants) retiennent notre attention. La première est neuve : la nomination par le responsable en interne d'un délégué à la protection des données. On peut le concevoir comme unique pour l'ensemble du pouvoir judiciaire ou comme multiple (par degrés de juridiction ou en fonction de l'application de tel ou tel texte ; sa tâche est ardue : en particulier, veiller au respect des prescrits des textes de protection des données et servir d'interface avec les personnes concernées.

24. La nomination d'un délégué – Tant le RGPD (article 37) que la Directive (article 32) obligent à la nomination, par le responsable, d'un délégué : *« 1. Les États membres prévoient que le responsable du traitement veille à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. 2. Le responsable du traitement aide le délégué à la protection des données à exercer les missions visées à l'article 34 en fournissant les ressources nécessaires pour exercer ces missions ainsi que l'accès aux données à caractère personnel et aux traitements, et lui permettant d'entretenir ses connaissances spécialisées. »* On note dans la Directive une exception (laissée à la discrétion des États membres) à cette obligation de nomination : *« Les États membres prévoient que le responsable du traitement désigne un délégué à la protection des données. Les États membres peuvent dispenser les tribunaux et d'autres autorités judiciaires indépendantes de cette obligation lorsqu'elles agissent dans l'exercice de leur fonction juridictionnelle. »* On s'étonne non point du contenu de la disposition, qui se justifie par la volonté de consacrer l'indépendance du juge dans sa fonction essentielle, celle de trancher le litige [30], mais du fait que cette exception trouve place dans un texte qui, en principe, n'est pas applicable à la fonction juridictionnelle (voir *supra*, n° 5).

25. La tenue d'un registre des traitements – On ne s'attardera pas à cette obligation prévue par l'article 30 du RGPD et par l'article 24 de la Directive. Il s'agit de publier une fiche d'identité reprenant les caractéristiques essentielles du ou des traitements opérés, de même que de son responsable voire de son ou ses sous-traitants : identité, finalités, base juridique, transferts, etc.

30 | On retrouve la même justification que celle donnée à la nécessité d'une autorité de contrôle propre aux traitements qui ressortissent à la fonction juridictionnelle (voir *supra*, n° 4).

26. La procédure d'évaluation des risques – Il s'agit de la procédure, préalable au traitement, qui consiste en une analyse d'impact du traitement, c'est-à-dire tant de l'évaluation des risques d'atteinte à la protection des données que de la motivation des solutions prises pour les minimiser. Le suivi de cette procédure est, selon l'article 35 du RGPD : *« Lorsqu'un type de traitement, en particulier par le recours aux nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un* ***risque élevé*** *pour les droits et les libertés des personnes physiques, les États membres prévoient que le responsable du traitement effectue* ***préalablement*** *au traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. »* Le devoir d'évaluation des risques encourus par la personne concernée est donc limité aux traitements à haut risque, dans lesquels il me semble qu'on peut ranger les serveurs de communications internes et externes reprenant les pièces de la procédure et les échanges de conclusions. La banque de données internes nominatives conservée et utilisée au sein des juridictions mérite également protection.

À raison même de leurs fonctions, les services et autorités couverts par la Directive sont concernés bien plus encore par l'obligation d'évaluation, à tel point que l'article 27 de la Directive contraint les États membres à imposer cette évaluation aux autorités en charge de la prévention, de la détection et de la poursuite des infractions pénales chaque fois que le recours aux nouvelles technologies (et on pense bien évidemment à l'intelligence artificielle et à des applications comme celles de reconnaissance faciale ou d'analyse génétique), la nature, le contexte et les finalités du traitement créent un risque élevé vis-à-vis des personnes, objet du traitement. L'article 28 exige en outre la consultation préalable de l'autorité de contrôle et son avis écrit préalable au démarrage du traitement : *« Les États membres prévoient que, lorsque l'autorité de contrôle est d'avis que le traitement prévu, visé au paragraphe 1 du présent article, constituerait une violation des dispositions adoptées en vertu de la présente directive, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'autorité de contrôle fournit par écrit, dans un délai maximum de six semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement,* ***et le cas échéant au sous-traitant,*** *et elle peut faire usage des pouvoirs visés à l'article 47. »*

On note que ce devoir d'évaluation concerne le responsable mais implique la coopération du sous-traitant à cette évaluation et peut entraîner une enquête auprès de ce dernier par l'autorité de contrôle. Ce point est important dans la mesure où, comme nous l'avons dit, nombre de traitements opérés par les tribunaux sont développés et gérés par des sociétés tierces.

27. Le droit des personnes concernées de ne pas être soumises à une décision automatisée – La quatrième obligation mériterait à elle seule un long exposé : elle concerne les **décisions automatisées** que le tribunal ou le parquet pourraient prendre. On parle de juge-robot, dont

on vante les qualités d'objectivité et d'efficacité, telles qu'il pourrait remplacer avantageusement le juge humain [31]. De même, au parquet, on peut imaginer que les systèmes experts ou d'intelligence artificielle facilitent voire remplacent les difficiles devoirs d'enquête de nos policiers et parquets. Ainsi, on vise le remplacement du juge par un système d'IA pour calculer les risques de récidive, l'indemnité à verser à la victime en cas d'accident, voire au-delà dans toute affaire, mais cela pourrait être également la mise sur pied d'un système de reconnaissance faciale mis en place pour détecter les suspects et les forcer à comparaître. Le RGPD et la Directive obligent à une information sur la « logique suivie », mais que veulent dire ces termes quand on sait que les algorithmes d'intelligence artificielle fonctionnent non sur des raisonnements causals mais simplement sur des corrélations non nécessairement prévisibles entre certaines données et que, dans les systèmes dits de *« deep learning »*, l'opacité des chemins découverts par l'ordinateur et la complexité des rapprochements suivis et opérés sont telles que même les concepteurs ne peuvent les comprendre et les formuler. Enfin, reconnaissons que le fait de donner une information *a priori* sur le système de décision risque de décevoir le justiciable qui souhaiterait comprendre comment l'ordinateur en est arrivé à la conclusion qui lui est opposée, et ce pour pouvoir se défendre. Ne peut-on dès lors exiger, au regard de l'exigence de motivation, c'est-à-dire d'intelligibilité des décisions prises par les autorités publiques et en particulier judiciaires, que les systèmes utilisés par les autorités tant policières que juridictionnelles soient transparents et qu'en toute hypothèse ils puissent être compris par le justiciable ?

Par ailleurs, si le RGPD et la Directive affirment certes le principe de la non-suffisance de cette « vérité » sortie des ordinateurs, ces dispositions du RGPD, en particulier celle de l'article 22, et de la directive contiennent de nombreuses ambiguïtés et soulèvent dès lors de nombreuses questions. Que veut dire « décision fondée exclusivement » ? À partir de quand pourra-t-on considérer que l'humain a une réelle capacité de remise en cause de la présomption de vérité sortie des ordinateurs ? Faut-il interdire, comme en France [32], le juge-robot ou l'accepter, en tout cas pour certains types de litiges, comme en Estonie [33] ? Faut-il admettre la possibilité de

31| Sur ce point, voir notamment l'ouvrage de Van Den Branden déjà cité (note 2).

32| Article 10 devenu article 21 de la loi française du 20 juin 2018 relative à la protection des données personnelles : *« Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne. Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage. »*

33| Qui, selon les propos tenus par le président de la Cour d'appel d'Estonie, vaudrait pour les litiges de petit montant.

« jugement d'avant-dire droit émis par la machine », mais contestable [34] ? Au-delà, ne faut-il pas exiger l'agrément de tout système d'IA d'aide à la fonction juridictionnelle au sens le plus large, y compris l'aide à la prévention et à la détection des infractions, la vérification de l'absence de biais, d'erreurs, et l'exigence d'une transparence des algorithmes [35] ? Agrément, oui, mais par qui ? Quand l'article 22 du RGPD réclame que l'utilisation de systèmes de décision automatisée requière pour être acceptable des « garanties appropriées » pour la personne concernée, que recouvrent ces termes : le droit à une audience explicative en face à face, un droit de contestation de la décision après explication ?

E. Les autorités de contrôle

28. Deux mots enfin sur cette ou ces autorités de contrôle – On rappelle que l'indépendance du judiciaire a conduit le législateur européen à affirmer le besoin d'autorités de contrôle spécifiques (*supra,* n° 4) [36]. Reste à fixer les conditions de leur indépendance, ce qui suppose des moyens techniques et humains, mais également la qualité d'expertise et d'indépendance des membres. Sans doute la question est-elle de savoir si on considère, en ce qui concerne le pouvoir judiciaire, qu'il est nécessaire de prévoir une ou plusieurs autorités de contrôle. On évoque ici l'intérêt de distinguer les juridictions de fond et la cour suprême. On évoque également l'idée d'autorités de contrôle distinctes suivant qu'il s'agit d'autorités du pouvoir judiciaire soumises à la Directive et non pas au RGPD. Ce point décidé, quelle composition proposer à cette ou ces autorités de contrôle ? Si le texte même des considérants évoque que l'autorité opère au sein du pouvoir judiciaire, le législateur serait sans doute avisé de confier le contrôle certes à des magistrats, mais également à des avocats voire à des représentants des justiciables. Ne serait-ce que par souci d'indépendance et de prise en considération des divers intérêts.

34 | C'est une des possibilités étudiées par D. MOUGENOT et L. GÉRARD, « Justice robotisée et droits fondamentaux », in Actes du colloque du 8 juin 2018 organisé par le CRIDS de l'université de Namur : *« Le juge et l'algorithme : Juges augmentés ou Justice diminuée ? »*, Larcier, 2019, p. 13 et s.

35 | Sur ces risques, O. LEROUX, « Justice pénale et algorithmes », in Actes du colloque du 8 juin 2018 organisé par le CRIDS de l'université de Namur : *« Le juge et l'algorithme : Juges augmentés ou Justice diminuée ? »*, Larcier, 2019, op. cit., 55 et s. p.; D. J. STEINBOCK, « Data Matching, Data Mining, and Due Process », *Georgia Law Review*, 2005, p. 61, et D. KEHL, P. GUO, S. KESSLER, « Responsive Communities, Algorithms in the Criminal Justice System : Assessing the Use of Risk Assessment in Sentencing », disponible en ligne : https://dash.harvard.edu/bitstream/handle/1/33746041/201707_responsivecommunities_2.pdf?sequence=1.

36 | Ainsi, l'APD mise en place par le législateur national ne pourrait contrôler les opérations effectuées par les juridictions *« dans l'accomplissement de leur fonction juridictionnelle »*. Dans son avis relatif au texte du RGPD, le Contrôleur européen de la protection des données (CEPD) (avis 6/2015) souhaite que les termes *« dans l'accomplissement de leur fonction juridictionnelle »* ne fassent pas l'objet d'une interprétation large mais visent uniquement les *« activités purement judiciaires »*.

Quant à leurs missions et compétences, elles sont largement définies : contrôle, y compris de la licéité, des traitements, sensibilisation, aide aux personnes concernées, conseil sur les nouveaux traitements, prononcé de sanctions effectives, proportionnées et dissuasives, etc.

Conclusions

29. Des nouvelles procédures et organes à mettre en place et des questions à résoudre – Notre conclusion, dans un premier temps, se limite à épingler quelques questions rencontrées lors de notre analyse de l'application des textes européens de protection des données. Ainsi, on relève les questions suivantes :

- Comment tracer la frontière entre les applications respectives du RGPD et de la Directive ? Comment éviter le *« gap »* entre l'application de la Directive et celle du RGPD ?

- Comment aborder la question de l'anonymisation des décisions jurisprudentielles ? Dans quelle mesure peut-on et doit-on éviter la publication nominative des jugements par extraits ou sous une forme journalistique par la presse voire par les réseaux sociaux, sachant le principe de la liberté d'expression ?

- À propos de la notion de responsable et de sous-traitant, quand peut-on considérer qu'il y a responsabilité conjointe entre le pouvoir judicaire et d'autres institutions organisantes dans le choix des moyens voire dans la définition des finalités ? Comment aborder la sous-traitance et les exigences en ce qui concerne la qualité du sous-traitant et le contenu de la convention à conclure avec lui ? Comment doter le pouvoir judicaire d'une cellule d'experts capable de définir les cahiers des charges et d'en contrôler la bonne exécution ?

- Quid des exceptions admises par la Directive aux principes de la protection des données (exactitude, pertinence, finalités compatibles) ? Jusqu'où peut-on admettre des règles nationales différentes en la matière ?

- Quelle(s) APD consacrer ? Quelle composition ? Jusqu'où doivent-elles être compétentes?

- Faut-il interdire ou limiter la prise de décisions sur une base totalement automatisée (idée du juge - robot) ? Faut-il exiger la transparence des algorithmes utilisés en toute hypothèse et quelle précaution prendre pour permettre la contestation de la décision projetée ? Au-delà, comment contrôler la qualité des systèmes d'aide à la décision utilisés par les parties voire par le juge ? Comment contrôler l'absence d'erreurs ou de biais ?

- Quand faut-il procéder à une analyse d'impact ?
- Quid de l'intervention de l'autorité de contrôle dans le cours de la procédure d'instruction ?

Des réponses nationales sont prévues pour la plupart de ces questions, certes, mais quid de la cohérence au niveau européen (par exemple : qui est responsable, durée de conservation, etc.) ? Ne faut-il pas, avec la collaboration des autorités de contrôle qui pourraient émerger des législations nationales, prévoir des *guidelines* communes afin d'assurer une certaine cohérence des réponses nationales ? Dans cet effort de cohérence, quel rôle pourraient jouer les juridictions européennes, qui pourraient fournir des modèles aux législateurs nationaux ? L'exemple récent d'Eurojust nommant un délégué et précisant les droits des personnes concernées est un premier pas en ce sens qui peut guider nos parquets.

Ce qui en tout cas apparaît évident, c'est **que la maîtrise par le pouvoir judiciaire de la numérisation de son fonctionnement exige ABSOLUMENT la création en son sein d'un organe comprenant des informaticiens et des gestionnaires qui puissent conseiller les magistrats dans le choix des moyens numériques** [37]**. Les textes européens en matière de protection des données appellent à cette maîtrise**.

30. Les principes généraux déduits du *« 'fair trial »* de l'article 6 du Conseil de l'Europe [38] – Le second point de nos conclusions élargit le débat. En quoi la numérisation de nos tribunaux met en danger les principes mêmes d'une bonne justice ? Distinguons les différents principes auxquels l'article 6 renvoie :

- **L'indépendance des magistrats** : le premier principe est la nécessité de l'indépendance à la fois de l'organisation judiciaire et des magistrats. Sans souligner ici les craintes

37| *« L'évolution technologique en question [l''utilisation de l'IA par les tribunaux] survient par ailleurs dans le contexte de l'autonomie de gestion du pouvoir judiciaire, dont les premières étapes ont été franchies suite à l'entrée en vigueur de la loi du 18 février 2014. Le Collège des Cours et Tribunaux et le Collège du Ministère Public, appelés à devenir les organes dirigeants de l'ordre judiciaire (à l'exception de la Cour de cassation), doivent se voir remettre les clés de l'évolution numérique. Même s'ils ne sont, pour l'instant, pas demandeurs que la gestion de l'ICT leur soit transférée , ils doivent être étroitement associés aux différentes étapes de la digitalisation de la justice et, a fortiori, à la création d'une institution « algorithmiste » considérée comme nécessaire par plusieurs intervenants. À défaut, le pouvoir judiciaire aura définitivement été privé de l'indépendance qui doit le caractériser. »* (D. MOUGENOT-L. GÉRARD, « Justice robotisée et droits fondamentaux », in Actes du colloque du 8 juin 2018 organisé par le CRIDS de l'université de Namur : *« Le juge et l'algorithme : Juges augmentés ou Justice diminuée ? »*, Larcier, 2019, p.13 et s.)

38| Sur les droits dits de procédure fondés sur l'article 6, paragraphe 1, de la Convention du Conseil de l'Europe, lire F. SUDRE, *Droit européen et international des droits de l'homme*, 14e éd., PUF, Paris, 2019, p. 379 et suivantes, et la bibliographie sur les diverses facettes de ce droit (no 450 de l'ouvrage) À noter l'arrêt de la Cour EDH du 13 septembre 2016, Ibrahim et autres c. Royaume-Uni (CE:ECHR:2016:0913JUD005054108), qui affirme que *« le droit à un procès équitable, consacré par l'article 6 § 1, ne souffre aucune dérogation »*.

de certains magistrats vis-à-vis de la numérisation utilisée comme outil de contrôle de l'activité et de la productivité des magistrats, on retient par contre comme risque majeur l'utilisation de systèmes d'intelligence artificielle pour remplacer ou simplement contrôler la « qualité » des jugements rendus et, à travers ce contrôle, la crainte d'une soumission du juge à l'interprétation majoritaire et à une normalisation des jugements, toute dissonance de raisonnement pouvant être perçue comme une « faute ». Enfin, l'introduction du numérique dans nos tribunaux crée un risque de dépendance du pouvoir judiciaire vis-à-vis de leurs fournisseurs privés, sans contrôle réel et effectif des algorithmes livrés, de leur pertinence et, le cas échéant, de leurs biais [39]. Mougenot [40]écrit : *« L'examen de nombreux contrats passés entre l'administration (de la Justice) américaine et des prestataires privés indique que, bien souvent, le fournisseur privé présente au gouvernement un contrat dans lequel la propriété et/ou la maîtrise des résultats appartient au prestataire. Combiné avec l'opacité du fonctionnement du système, cela signifie que les pouvoirs publics perdent la maîtrise du processus et de son résultat. On assiste alors à un déplacement de l'imputabilité de l'acte de juger du public vers le privé, même si, sur papier, le jugement reste un produit de l'État. »*

- La publicité de l'audience et du prononcé constitue un moyen pour le citoyen de s'assurer du respect de la loi et du respect de la procédure. Peut-on considérer que la publication rapide du jugement qu'autorise le numérique le soit au nom de l'efficacité et de la disparition de l'audience et du prononcé ?

- Le droit d'être entendu est une garantie essentielle pour le justiciable. *A priori*, l'affirmation de ce droit condamne toute décision automatisée et réclame que, même si des systèmes experts ou d'intelligence artificielle peuvent aider le juge dans son processus décisionnel, il est absolument requis qu'il puisse rencontrer et entendre physiquement les parties (voir *supra,* n° 27, nos commentaires sur l'interdiction par l'article 22 de décisions fondées exclusivement sur un système automatisé).

- La motivation des jugements constitue une autre garantie pour les justiciables. Elle oblige les juges à répondre point par point aux arguments avancés par les parties. Elle implique en outre que les justiciables doivent pouvoir comprendre le raisonnement du

39| Ainsi, il est à craindre que les systèmes d'intelligence artificielle n'utilisent, surtout dans les pays où le nombre de jugements est loin d'être suffisant pour créer la *« big data »* nécessaire, des jugements étrangers basés sur d'autres législations.

40| D. MOUGENOT et L. GÉRARD, op. cit., p. 55 et s.; cf. également sur ce point les remarques sévères de A. GARAPON et J. LESSEGUE, *Justice numérique*, Paris, PUF, 2018, p. 86.

juge tant en ce qui concerne la décision que la peine fixée [41] et ainsi pouvoir le contester, le cas échéant. Dans le cas d'utilisation des systèmes automatisés d'aide à la décision voire de décision purement automatisée, il importe, afin d'assurer au mieux le droit à la motivation des décisions de justice, que tout justiciable puisse, sans démarche de sa part, obtenir communication, dans un format intelligible, de l'explication de la décision en même temps que la décision elle-même. En outre, si la communication d'une explication était jugée non suffisante pour la compréhension par le justiciable du jugement ou de la proposition de jugement à son égard, le droit d'exiger du bénéficiaire à une explication orale fournie par un humain devrait être envisagé.

- L'égalité des armes et, *a fortiori*, l'accès aux prétoires, qui conditionne la possibilité de se défendre, pourraient être mis en cause du fait que l'accès aux multiples services payant à haute valeur ajoutée que permet la numérisation pourrait s'avérer difficile à des justiciables qui ne pourraient se payer les services de cabinets d'avocats ou de consultants ayant pignon sur rue et suffisamment bien équipés pour disposer de ces ressources informationnelles. En particulier, l'accès à de vastes quantités de données présentes dans le dossier et leur traitement et, plus encore, l'analyse automatique des « précédents » et des textes législatifs ou le calcul des chances de réussite permettent à ceux qui disposent de tels outils de bénéficier d'avantages sur la partie adverse qui en est dépourvue [42]. Comme le note un arrêt de 2010 de la Cour de Luxembourg [43] à propos des restrictions d'accès possibles que représentait l'obligation de passer par la voie électronique pour pouvoir bénéficier d'une conciliation judiciaire, *« l'exercice des droits conférés [...] pourrait être rendu pratiquement impossible ou excessivement difficile pour certains justiciables, et notamment ceux ne disposant pas d'un accès à Internet, s'il ne pouvait être accédé à la procédure de conciliation que par la voie électronique ».* Que dire alors des risques de discrimination entre justiciables créés par les nouvelles applications citées plus haut... La numérisation de la justice signifie un déséquilibre croissant entre le pouvoir de ceux qui, financièrement et intellectuellement, disposent de l'équipement nécessaire pour avoir accès à l'information nécessaire et des moyens de la traiter et ceux qui ne l'ont pas, y compris les magistrats [44]. N'y-a-t-il pas urgence à créer un service

41 | Ce sont les fameux arrêts de la Cour EDH du 16 novembre 2010, Taxquet c. Belgique (CE:ECHR:2010:1116JUD000092605), et du 29 novembre 2016, Lhermitte c. Belgique (CE:ECHR:2016:1129JUD003423809).

42 | À propos des multiples services offerts désormais par le numérique aux *legaltechs*, lire, entre autres, O. CHADUTEAU, « Panorama des legaltechs – Les métiers du droit au défi du numérique », *Enjeux numériques – Annales des Mines*, nº 3 – Septembre 2018.

43 | Arrêt du 18 mars 2010, *Alassini e.a.*, C-317/08 à C-320/08, EU:C:2010:146, point 58.

44 | Généralement privés pour des raisons budgétaires de l'accès aux ressources du numérique...

universel gratuit d'accès électronique non seulement aux données jurisprudentielles brutes, mais encore à des services d'interrogation sémantique de ces données brutes, de manière à pallier le risque ainsi dénoncé [45] ?

31. Un appel à la vigilance – Ainsi, il est permis de conclure notre propos non par un refus de la numérisation de nos parquets et de nos tribunaux, mais simplement par un appel à la vigilance. L'efficacité [46], la réduction des coûts [47] voire la qualité du travail qu'apporte l'utilisation des technologies, y compris de l'intelligence artificielle, ne peuvent distraire nos magistrats, nos officiers de police judiciaire et membres du parquet partout et toujours de veiller au respect, d'une part, des principes fondamentaux de la Justice dans un pays démocratique et, d'autre part, de la vie privée des justiciables. C'est ainsi que la Charte éthique élaborée par le CEPEJ [48] va plus loin, dans la mesure où elle exige que pour tous les traitements fonctionnant à l'aide de systèmes IA, « qu'ils soient conçus dans le but d'apporter un support à une consultation juridique, une aide à la rédaction ou à la décision ou une orientation des justiciables, il est essentiel que lesdits traitements soient effectués dans des conditions de transparence, de neutralité et de loyauté certifiées par une expertise extérieure à l'opérateur et indépendante ».

45| Cf. à cet égard nos conclusions du colloque du 8 juin 2018 organisé par le CRIDS de l'université de Namur : *« Le juge et l'algorithme : Juges augmentés ou Justice diminuée ? », Larcier, 2019 : « Comme le note la juge MESSIAEN : "On ne rappellera jamais assez que la justice n'est pas un 'business', une 'organisation de service orienté client' , n'en déplaise au Ministre. La justice doit rester un service public, qui doit pouvoir atteindre et rester accessible aux plus faibles, afin de leur assurer une place dans la société en les traitant avec dignité et considération. " Ce service public se fonderait sur le principe de l'égalité des armes, un service d'accès à des outils d'IA qui pourrait être offert à tous et à chacun : cabinets d'avocats, entreprises, administrations et citoyens sans oublier nos tribunaux, doivent également pouvoir lutter à armes égales avec l'Intelligence des plaideurs, surtout lorsqu'elle est artificielle. Avant de conclure sur le besoin d'étendre le service public du conseil juridique au regard de l'IA et de son contenu, il importera en tout cas d'examiner l'impact de l'utilisation de l'IA dans le secteur du droit, sa généralisation auprès d'associations comme les syndicats, les associations de consommateurs ou de libertés civiles. »*

46| Sur l'ambiguïté du terme « efficacité » et ses relations avec les NTIC, lire J. MAIA, « L'efficacité du droit et les nouvelles technologies, in *L'E-justice – Dialogue et Pouvoir, Arch. de philos. du droit, no 54*, Dalloz, p. 7 et suivantes.

47| C'est du moins ce que conclut la COMMISSION eUROPEENNE pOUR l'eFFICACITE dE lA jUSTICE *dans ses Lignes directrices sur la conduite du changement vers la cyberjustice : Bilan des dispositifs déployés et synthèse de bonnes pratiques* (adoptées le 7 décembre 2016, Conseil de l'Europe, juin 2017) *: « [Pour un] nombre équivalent d'affaires traitées, un juge-robot présente un coût largement moindre à celui d'un juge humain. »*

48| Il s'agit de la charte éthique élaborée par la Commission européenne pour l'efficacité de la justice du Conseil de l'Europe, qui, lors de sa réunion des 3 et 4 décembre 2018, a adopté la *Charte européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement*, https://www.coe.int/fr/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment.

Elle énonce par ailleurs cinq principes d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement :

> *« – PRINCIPE DE RESPECT DES DROITS FONDAMENTAUX : assurer une conception et une mise en œuvre des outils et des services d'intelligence artificielle qui soient compatibles avec les droits fondamentaux.*
>
> *– PRINCIPE DE NON-DISCRIMINATION : prévenir spécifiquement la création ou le renforcement de discriminations entre individus ou groupes d'individus.*
>
> *– PRINCIPE DE QUALITÉ et SÉCURITÉ : en ce qui concerne le traitement des décisions juridictionnelles et des données judiciaires, utiliser des sources certifiées et des données intangibles avec des modèles conçus d'une manière multidisciplinaire, dans un environnement technologique sécurisé.*
>
> *– PRINCIPE DE TRANSPARENCE, DE NEUTRALITÉ ET D'INTÉGRITÉ INTELLECTUELLE : rendre accessibles et compréhensibles les méthodologies de traitement des données, autoriser les audits externes.*
>
> *– PRINCIPE DE MAÎTRISE PAR L'UTILISATEUR : bannir une approche prescriptive et permettre à l'usager d'être un acteur éclairé et maître de ses choix. »* [49]

32. Pour une justice et une intelligence humaines – Au-delà, il vous est demandé de préserver, mieux : de promouvoir, une **justice humaine, celle mise en œuvre par une intelligence proprement humaine capable d'écoute des justiciables et de discuter voire s'opposer aux vérités que lui dicterait l'ordinateur** [50]. Le droit est prudence, il est incertitude au service des hommes, mais cette incertitude n'est pas pur flou ; elle se mesure à l'aune d'une certitude, celle de textes réglementaires légalement adoptés et publiés. À l'inverse des "lois" inscrites dans les programmes informatiques et jamais contestables parce qu'écrites en mode binaire et non transparent, ces textes ouvrent, comme tout langage humain, des possibles et jamais

49| Cette exigence va dans le sens d'autres rapports européens qui plaident nettement en faveur d'une obligation pour des systèmes d'IA ayant un impact sur la situation d'individus d'être soumis à des audits extérieurs fondés sur certains principes éthiques afin qu'ils soient *« trustworthy »*.

50| Nous faisons ici l'apologie du « revirement de jurisprudence » : *« Les exigences de la sécurité juridique et de protection de la confiance légitime des justiciables ne consacrent pas un droit acquis à une jurisprudence constante »* (Unedic c. France, 18 décembre 2008, J.C.P. G, 2009, note F. SUDRE). On note que la reconnaissance du principe de distinction en Angleterre ouvre de même aux juges anglais l'échappatoire nécessaire à l'application de la règle du précédent.

n'enclosent complètement la décision [51]. Le droit n'est jamais certitude mathématique [52], il est devoir d'interprétation des textes confrontés à des faits et des hommes. N'est-ce pas là la ignité de votre fonction, Mesdames et Messieurs les magistrats ? Il est bon de le rappeler en ce beau jour d'anniversaire.

51 | Comme le relève la professeure M. HILDEBRANDT [« Law as computation in the era of artificial legal intelligence : Speaking law to the power of statistics » (2018) 68 : supplément 1 UTLJ 12, à la p. 23], il y a une dimension interprétative du droit qui est rétive à toute forme d'automation : *« Whereas machines may become very good in such simulation, judgment itself is predicated on the contestability of any specific interpretation of legal certainty in the light of the integrity of the legal system, which goes way beyond a quasi-mathematical consistency. »*

52 | Cf. dans le même sens, parmi d'autres, D. BOURCIER, « L'acte de juger est-il modélisable ? De la logique à la justice », *L'E-justice – Dialogue et Pouvoir, Arch. de philos. du droit*, no 54, Dalloz, p. 37 et suivantes.