# Pas de pardon au paradis du numérique ?

Poullet, Yves

*Published in:*
De la récidive au pardon

*Publication date:*
2021

*Document Version*
le PDF de l'éditeur

# Pas de pardon au paradis du numérique ?

© Yves Poullet

Professeur associé à l'UCLille

Recteur honoraire de l'Université de Namur

Membre de l'académie royale de Belgique

***« Even if it become possible in centuries to come for machines to replace aspects or all of the judicial function, would this be morally and socially desirable ? »***

**(**R. SUSSKIND, *The future of Law*, Oxford University Press, 1996, p. 69**)**

## Introduction

1. **Deux cas emblématiques – L'affaire Lloomis et l'affaire Google** – L'affaire Loomis[1] est connue. Le 11 février 2013, un cambriolage est commis dans l'Etat du Wisconsin. Un des auteurs, Mr Lloomis est arrêté et condamné. Rien que de très normal, me direz-vous. La particularité de la condamnation sévère tient au fait que le tribunal américain - et le point est confirmé en cour d'appel - tient compte du risque de récidive présenté par Lloomis, tel qu'il est attesté par l'utilisation du système dit d'intelligence artificielle dit COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions)*[2]. On note que le système[3] a été développé par une société privée Northpointe

[1] Sur cette affaire, lire l'ouvrage provocant mais inspirant de A. Vandenbranden, *Les robots à l'assaut de la Justice*, Larcier, 2018. En ce qui concerne l'existence de biais et en pariculier vis-à-vis des populations noires voir le rapport de l'organisation PROPUBLICA (Julia Angwin, Jeff Larson, Surya Mattu et Lauren Kirchner) :. « *Machine Bias. There's software used accross the country to predict future criminals. And it's biased against blacks Our analysis of Northpointe's tool, called COMPAS (...), found that black defendants were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than black defendants to be incorrectly flagged as low risk* », (23 mai 2016), ProPublica (blogue), en ligne : https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing ")

[2] Outre le système COMPAS, on note l'utilisation d'un autre système d'intelligence artificielle, PREDPOL, qui aide les services de police à prévenir les risques de crimes graves. Le site de cette société énonce comme suit les services Sur son site internet, la société PredPol évoque comme suit les services offerts : « *PredPol services police departments and sheriff agencies around the United States as well as internationally (...) The company is privately held* ».

[3] Ce système croise des réponses à des questionnaires (plus de 150 items) et des données psycho-socio-économiques relatives à la personne, au milieu de vie, etc. Il est à noter que les algorithmes sont protégés par un

Ainsi, c'est l'ordinateur qui 'juge' et les tribunaux humains s'en remettent à la vérité proclamée par un ordinateur dont on note qu'il n'est pas exempt de biais[4] et a été développé par une société privée sans contrôle de nos 'juges'. Le second cas est l'affaire Google Spain jugée par la CJUE en grande chambre, le 13 mai 2014[5]. En deux mots, un citoyen espagnol, M. Costeja González avait introduit auprès de l'agence espagnole de protection des données, une plainte à l'encontre tant du quotidien *La Vanguardia* que de Google. Sa réclamation se fondait sur le fait qu'une recherche de son nom auprès du célèbre moteur de recherche aboutissait à l'affichage de liens vers deux pages du site web de *La Vanguardia*. Ces pages mentionnaient son nom en lien avec une vente aux enchères immobilière suite à une saisie pratiquée en recouvrement de dettes de sécurité sociale. La demande adressée à *La Vanguardia*, réclamait la suppression ou, à tout le moins, la modification des pages incriminées afin que ses données personnelles n'y apparaissent plus ; la demande envers Google portait sur la suppression des liens entre son nom et le site de *La Vanguardia*. L'agence espagnole fit droit non à la demande envers le journal mais bien envers Google. Google fit appel de cette décision devant « l'*Audiencia Nacional* », qui posa plusieurs questions préjudicielles à la Cour de justice de l'Union européenne. En particulier, il s'agissait de savoir si, compte tenu de la liberté d'expression à laquelle Google participait en assurant une diffusion singulièrement élargie à la publication légitime par un journal local d'une information relative à une condamnation, l'AEPD était en droit d'exiger suite à la demande de la personne intéressée, le 'déférencement' par Google de certaines pages web.

2. **Au-delà des affaires – les risques dénoncés** - Ainsi, l'ordinateur si on n'y prend garde, nous profilera comme suspect, potentiel criminel ou récidiviste. Ce qui est à craindre, c'est que le profilage proposé soit pris comme argent comptant et conduise, comme dans l'affaire Lloomis, à des décisions qui à la limite pourront se passer du jugement humain. Par ailleurs, il est à craindre que, dans la mémoire sans limite de nos ordinateurs, la stigmatisation ne devienne éternelle et élargie aux dimensions de l'univers comme le démontre les faits à l'origine de l'affaire Google, là où le droit exige le pardon social qu'offrent la prescription[6] ou la réhabilitation. Ces risques notés, tout n'est pas noir au pays de la justice devenue numérique. 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

---

droit d'auteur et un secret d'affaires qui en protège la divulgation et interdit toute transparence sur les corrélations qui permettraient d'expliquer la décision, en l'occurrence la présence d'un risque de récidive.

[4] Ainsi, l'analyse du fonctionnement des algorithmes révèle que le logiciel a une tendance à considérer que les noirs sont plus criminogènes que les blancs.

[5] CJUE, 13 mai 2014, Google Spain c. AEPD et Maria Costeja Gonzales, C.131/12. Parmi de nombreux commentaires, lire C. de Terwangne, Droit à l'oubli, droit à l'effacement ou droit au déférencement ? Quand le législateur et les juges européens dessinent les contours du droit à l'oubli numérique, *Le droit à l'oubli numérique*, Bruxelles, Larcier, 2015, p. 270.

[6] Gérard Cornu définit le concept comme étant un « *Mode d*acquisition ou d*extinction d'un droit, pour l'écoulement d'un certain laps de temps (d'un *délai) et sous les conditions déterminées par la loi (C. civ., article. 2219 ancien.)* » La notion de prescription est présente dans de nombreuses branches du droit, a l'instar du droit penal87 et du droit civil. En France, la prescription en matière pénale distingue la prescription liée au droit de poursuite, telle que définie par la *Loi n°2017-242 du 27 février 2017 portant réforme de la prescription en matière pénale, JORF n°0050 du 28 février 2017*; et la prescription appliquée à la peine. Ainsi, l'article 133-2 du Code pénal dispose que « *Les peines prononcées pour un crime se prescrivent par vingt années révolues à compter de la date à laquelle la décision de condamnation est devenue définitive* ». L'article 133-3 dispose que : « *Les peines prononcées pour un délit se prescrivent par six années révolues à compter de la date à laquelle la décision de condamnation est devenue définitive* ». Enfin, l'article 133-4 dispose que : « *Les peines prononcées pour une contravention se prescrivent par trois années révolues à compter de la date à laquelle la décision de condamnation est devenue définitive* »

l'élucidation des affaires est évidente : plus de 70 pour cent 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 par la police et les parquets des outils du numérique. Ces apports ont des limites. Notre contribution en pointe une source en particulier : les textes européens récents en matière de protection des données : la directive 2016/680[7] sur les traitements relatifs aux infractions pénales[8] que le titre III de la loi française du 20 juin 2018[9]transpose dans les articles 70 et s. de la loi 'Informatique et Libertés'.

3. **Un rapide survol du propos –** Il s'agit donc d'analyser brièvement les diverses dispositions de cette directive et de sa transposition nationale permettent de diminuer voire supprimer les risques dénoncés liés tantôt aux méthodes de profilage[10] utilisés aux divers stades de la procédure que comme support aux décisions qu'aux possibilités de stockage et de diffusion illimitées des suspicions et incriminations pénales au-delà des décisions de justice[11]. Notre analyse suivra la distinction proposée :
    - le profilage et autres traitements par les autorités publiques aux divers stades de l'enquête et la directive de protection des données 2016/680;
    - le stockage et la diffusion des données liées à des infractions pénales et la directive en dehors des autorités publiques.

## I. Les traitements en particulier de profilage aux divers stades de l'enquête et la directive de protection des données 2016/680

4. **Les traitements visés par la Directive -** Les dispositions de la directive comme des articles 70 et s. de la loi française s'appliquent à tout traitement de données à caractère personnel mis en œuvre, 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.

---

[7] 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.

[8] 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 (éds), Cahier du CRIDS, n° 44, 2018, p. 865 et s.

[9] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles**,** JORF du 21 juin 2018

[10] Le RGPD définit le profilage à l'article 4 (4) comme suit : « «profilage», « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique*. » La 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 des données reprend la même définition en son article 3(4).

[11] Exceptionnellement, en raison de son champ d'application restreint aux « missions juridictionnelles » des autorités juridictionnelles y compris en matière pénale, nous devrons également nous référer au RGPD. Sur ces délicates questions de frontière entre l'application en matière de procédure pénale du RGPD versus l'application de la Directive, notre contribution : « Les tribunaux à l'heure du numérique et … des législations de protection des données: de quelques zones d'incertitude » in *Actes du colloque « LE TRIBUNAL DE L'UNION EUROPÉENNE À L'ÈRE DU NUMÉRIQUE »*, Luxembourg, le 24 septembre 2019 (à paraître)

Deux points : le premier porte sur le fait que les traitements au sein de la police et du parquet peuvent être développés tant à des buts préventifs que répressifs ; le second concerne la notion d''infraction pénale', définie largement par la CJUE[12] 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.

Le premier point est important. De plus en plus, l'utilisation par les autorités policières en collaboration avec d'autres autorités ou non de systèmes d'intelligence artificielle permet de prévenir les crimes[13]. On sait que le Danemark a ainsi mis au point un logiciel qui permet de repérer *a priori* les familles où les risques d'enfants battus ou délaissés sont importants[14], que d'autres pays profilent en fonction de critères socio-économiques les futurs criminels[15]. Au parquet, on peut ainsi imaginer que les systèmes experts ou

---

[12] Le considérant n° 13 rappelle ainsi la jurisprudence de la CJUE, en particulier l'arrêt du 27 mai 2014 dans l'affaire Zorian Spacic.

[13] Ainsi, par exemple, le système I-Border Ctrl actuellement développé par l'Europe pour le contrôle des frontières, dont les modules sont décrits comme suit par le rapport d'Algorithmwatch et de la fondation Bertelsman (*Automating Society Taking Stock of Automated Decision-Making in the EU, A report by AlgorithmWatch in cooperation with Bertelsmann Stiftung*, supported by the Open Society Foundations, Janvier 2019): *« **An Automatic Deception Detection System (ADDS)** that performs, controls and assesses the pre-registration interview that is personalised to suit the gender and language of the traveller. ADDS quantifies the probability of deceit in interviews by analysing interviewees' non-verbal micro expressions ; **a Biometrics Module** for the biometric identity validation, comparing data stored in databases (legacy systems in the case of fingerprints and creation of a baseline database for palm vein images) **; a Face Matching Tool (FMT),** including video and photo to create a biometric signature in order to provide a matching score ; a **Document Authenticity Analytics Tool (DAAT)** for the verification procedure of travel documents, which are examined by DAAT against fraud characteristics in an automated way. A matching score concerning the authenticity of documents is then derived ; **an External Legacy and Social interfaces system (ELSI),** crosschecking the traveller's information from social media or legacy systems, such as SIS II ; a **Risk Based Assessment Tool (RBAT),** utilising risk based approaches to intelligently aggregate and correlate all the data collected and the estimated risk. It then classifies travellers to support the decision of the border guard. This includes a systematic process to stimulate compliance by compressing all the data into meaningful actionable risk scores ; a**n Integrated Border Control Analytics Tool (BCAT)** for advanced post-hoc analytics ; **a Hidden Human Detection Tool (HHD)** to detect people inside various vehicles. iBorderCtrl states that "regarding the expected accuracy it would be wrong to expect 100% accuracy from any AI-based deception detection technology, no matter how mature". iBorderCtrl therefore relies "on many components that address various aspects of the border control procedures, and each provides its own risk estimation for the traveller". The system then "synthesises a single risk score from a weighted combination of components". Emphasising the "human-in-the-loop principle", the makers conclude that "it is highly unlikely that an overall system of which ADDS is a part will lead to 'an implementation of a pseudoscientific border control.'"*

[14] Soit le système dénommé Gladsaxe. Sur ce système, lire : JORGENSEN, R. F., Når informationsøkonomien bliver personlig (When Information Economy gets personal). In R. F. Jørgensen, & B. K. Olsen (red.), *Eksponeret: Grænser for privatliv i en digital tid*, Gad., 2018, p, 86 et s.

[15] On note que le profilage n'est pas nécessairement individuel mais peut concerner, dans un premier temps du moins, un groupe de personnes partageant des traits communs (la race, les caractéristiques d'éducation, les ascendances, le type de relations sociales, etc.). En d'autres termes, nous insistons sur la lacune que représentent en la matière les législations de protection des données à caractère personnel. Ces législations n'envisagent pas les risques 'collectifs' de discrimination, risques qui pourtant seront souvent présents dans le profilage policier. Sur les effets du profilage policier, en particulier celui illicite, sur la confiance des citoyens, lire le rapport de l'agence européenne des droits fondamentaux de décembre 2018, *Guide pour la prévention du profilage illicite aujourd'hui et demain*, disponible sur le site de l'agence : https://fra.europa.eu/fr/publication/2019/guide-pour-la-prevention-du-profilage-illicite-aujourdhui-et-demain

d'intelligence artificielle facilitent voire remplacent les difficiles devoirs d'enquête de nos policiers et parquets Comment aborder la réglementation de ces profilages ?

5. **Profilage et système automatisé de décisions individuelles -** Le profilage dans la mesure où il conduit à une décision comme c'était le cas dans l'affaire Lloomis[16] en ce qui concerne le calcul du risque de récidive[17]. D'autres affaires américaines ont depuis été jugées. On cite l'affaire Jordan Samsa convaincu d'avoir violé sa belle-sœur. Dans ce cas l'application du même logiciel COMPAS aboutissait à un résultat cette fois négatif et l'argument avait été invoqué en appel par les avocats du prévenu. Les juges d'appel[18] refusent l'argument : le dernier mot doit être donné au jugement humain et non à l'ordinateur. Dans le même sens, on citera l'attitude des juges de la Cour suprême de l'Indiana dans l'affaire Malenchick[19], où le résultat de l'algorithme avait été considéré comme une circonstance aggravante. Les juges de la Cour suprême rejettent une telle décision au motif que le système d'évaluation algorithmique n'avait aucune base scientifique et ne pouvait se substituer à un jugement humain[20].

   De manière plus large, le fait de répondre à un profil ou d'être 'épinglé' par un système d'intelligence artificielle[21] pourrait si on n'y prend garde conduire la police ou l'autorité du parquet à vous considérer comme suspect voire coupable. De telles conclusions constituent, au sens du RGPD et de la Directive, une décision fondée exclusivement sur un traitement automatisé... L'article 11. 1 de la Directive énonce à cet égard les règles suivantes : « *Les États membres prévoient que toute décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques défavorables pour la personne concernée ou l'affecte de manière significative, est interdite, à moins qu'elle ne soit autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis et qui fournit des garanties appropriées pour les droits et libertés de la personne concernée, et au minimum le droit d'obtenir une intervention humaine de la part du responsable du traitement. »*. On ajoute que les deuxième et troisième alinéas sont sévères quant à l'utilisation de données sensibles (race, religion, options syndicales, philosophiques, données de santé, …) en permettant toutefois également des exceptions mais en interdisant toute discrimination fondée sur de telles données[22].

6. **Les lacunes de la disposition européenne** - L'analyse de cette disposition laisse apparaître nombre de lacunes et en tout cas d'ambiguïtés. Que veut dire '*décision fondée exclusivement*' ? L'exception prévue par le texte est large dans la mesure où la Directive se réfère au 'droit' de l'Etat-membre et on sait combien cela peut s'entendre de sources bien éloignées des garanties offertes par la loi au sens strict et par le débat législatif que

---

[16] State of Wisconsin c. Eric Lloomis, 881 NWed 749, 2016, Supreme Court of Wisconsin

[17] O. LEROUX (« Justice pénale et algorithme », In le Juge et l'algorithme, Cahiers du CRIDS, n° 47, Larcier 2019, p. 63) décrit notamment le programme actuellement testé par la police de Durham (RU) appelé *Harm Assessment Risk Tool (HART),* qui aide la police à déterminer si un suspect doit ou non être repris dans un programme de réinsertion.

[18] State c. Samsa 859 NW 2d 149 (2014) Court of Appeal of Wisconsin.

[19] Anthony Malenchik c. State of Indiana, 928 NE éd 564, 575 (Ind. 2010), Indiana Supreme Court.

[20] Sur ces trois affaires américaines, lire C. PAPINEAU, *Droit et intelligence artificielle : essai sur la reconnaissance du droit computationnel,* Thèse, Université de Paris 1 Panthéon et Université de Montréal, à paraître, notamment p. 20 et s.

[21] Par exemple par un système de reconnaissance faciale mis en place pour détecter les auteurs d'infraction. Voir également le système PREDPOL décrit *supra,* note 2.

[22] Ainsi, dans l'affaire Llomis, il a été démontré que le système COMPAS avait progressivement pris en compte la race noire comme facteur d'aggravation des risques de récidive.

son adoption suppose. La décision doit s'adresser à une « personne concernée ». C'est la conséquence certes d'une législation centrée sur la protection de personnes individuelles mais ne faudrait-il pas également prendre en compte le fait que des systèmes en particulier prédictifs visent des catégories de personnes, ainsi les personnes habitant tel quartier, ayant tel type de comportement sur le net, telle mobilité…le risque est ici collectif mais mériteraient à notre avis *a fortiori* d'être pris en compte ?

Que recouvrent les termes '*garanties appropriées*' : le droit à une audience explicative en face à face ; un droit de contestation de la décision après explication ? Les '*garanties appropriées*' exigent t'elles que l'autorité policière, sans doute une fois l'enquête bouclée (secret de l'instruction oblige !), explique le raisonnement suivi qui a présidé à la suspicion ou à la mesure prise par l'autorité policière voire judiciaire ? Pas évident, ces dernières pourraient se contenter d'une vague explication sur les algorithmes à l'œuvre sans nécessairement en expliquer le fonctionnement et le résultat à la personne concernée dans son cas précis. D'autant moins évident que le concepteur en même temps souvent fournisseur du système (voir les cas de Northpointe et Predpol) est une entreprise privée et pourra exhiber de son droit au secret des affaires ou à la propriété intellectuelle. Enfin, on ajoute que, dans le cas de systèmes non supervisés dits de *deep learning*, la transparence du fonctionnement des algorithmes voire leur explicabilité deviennent difficiles sinon impossibles[23].

Enfin, toujours à propos des garanties, certes l'article exige *l''intervention humaine*' mais 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[24] ? On l'a compris, il faut plaider pour des systèmes d'intelligence artificielle au fonctionnement transparent même lorsque fourni par des tiers et pour la définition et l'imposition de bonnes pratiques organisationnelles afin de garantir de manière appropriée la réponse motivée[25] aux arguments de la personne concernée. Au-delà, ne faut-il pas exiger l'agrément *a priori* de tout système d'IA d'aide à la fonction juridictionnelle au sens le plus large c'est à dire y compris l'aide à la prévention et à la détection des infractions ? Il s'agira de procéder à la vérification de l'absence de biais, d'erreurs et l'exigence d'une transparence des algorithmes[26] ? Le point 7 reviendra sur ce point.

---

[23] « *Sur la transparence, il y a peut-être un élément négatif de la technologie actuelle, à savoir que la plupart de ces algorithmes d'apprentissage ne savent pas donner d'explications. Dans un contexte juridique, on s'attend à ce qu'on explique les décisions, pour que la personne comprenne, pour que cela puisse servir de modèle. Ceci est encore une limite de la technologie informatique actuelle et c'est pour cela qu'il y a certains cas dans lesquels on ne peut pas (…) l'utiliser* » (S. ABITEBOUL, « Table ronde n°1 – L'intelligence artificielle, outil ou révolution pour le monde du droit ?*», Colloque de l'Association Droit & Affaires, L'intelligence artificielle : enjeux de société et objet de droit, présenté au Sénat français, 16 mars 2018*, p. 115.

[24] Sur cette 'incontestabilité' de la décision produite par la machine, lire entre autres, M. KAMINSKY : "*And where human decision-making can often be contested, algorithmic decision-making (…) is often taken at face value, and left unchallenged and unchallengeable*. ». ("Binary governance: lessons from the GDPR's approach to algorithmic accountability", *Southern California Law Review*, 2019, 76, p. 15.

[25] Sur cette exigence de motivation au cœur des principes déduits de l'article 6 de la CEDH, parmi tant d'autres, lire L. GERARD et D. MOUGENOT, « 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. 29 et s.

[26] 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, 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

On rappelle enfin l'a*rticle 10 de la loi française qui trouvera à s'appliquer chaque fois qu'un juge d'instruction ou un magistrat devra prendre une décision : « -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.* ». Cet article a été repris par l'article 21 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles. Bref, à travers toutes ces remarques, il s'agit de veiller à ce que les garanties du « *fair trial* », exigé tant par l'article 6 de la CEDH que par l'article 47 de la Charte des droits fondamentaux de l'Union européenne instituant le droit à un recours effectif et à accéder à un tribunal impartial soit respecté : «*Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter. Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l'effectivité de l'accès à la justice.* »[27]

7. **La procédure d'évaluation des risques -** Deux autres dispositions de la Directive permettent d'entourer le profilage et constituent de réelles protections pour les personnes mises en cause à propos d'infractions pénales. La première vise les systèmes mis en place par les autorités policières et judiciaires. La Directive **impose aux pouvoirs policier et judiciaire une procédure d'évaluation des risques** : il s'agit d'une procédure, préalable au traitement, qui consiste en une analyse d'impact du traitement, c'est-à-dire tant d'évaluation des risques d'atteinte à la protection des données que de la motivation des solutions prises pour les minimiser. A raison même de leurs fonctions, les services et autorités couvertes 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 Etats 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 facile ou d'analyse génétique), la nature, le contexte et les finalités du traitement crée 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,*

ligne: https://dash.harvard.edu/bitstream/handle/1/33746041/201707_responsivecommunities_2.pdf?sequence=1. Cf. également la déclaration d'A. GARAPON (« Les enjeux de la justice prédictive », *La semaine juridique,* 2017, n°1-2, p. 13 : « *Si elle ne veut pas passer pour une justice divinatoire, aussi mystérieuse et intimidante que les oracles antiques, la justice prédictive doit rendre public ses algorithmes et ne pas se réfugier derrière le secret de fabrication.* »

[27] Pour une réflexion complète sur l'utilisation de l'IA dans les tribunaux au regard des principes du '*fair trial*' lire L. GERARD et D. MOUGENOT, « 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. 29 et s

*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 relèvera que l'autorité de contrôle aurait pu ne pas être la CNIL dans la mesure où latitude est laissée aux Etats membres de créer une autorité de contrôle spécifique aux traitements policiers et à ceux du parquet[28], cette latitude devenant obligation lorsqu'il s'agit des autorités juridictionnelles, en tout cas dans le cadre de l'exercice de leurs fonctions juridictionnelles[29].

Le devoir d'évaluation concerne, on le note, 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 nombre de traitements opérés par les tribunaux sont développés et gérés par des sociétés tierces. Au-delà, on dénonce la crainte de biais dus au fait que les concepteurs des algorithmes ne représentent qu'une partie infime de la population. Comme l'écrit Joy ITO, directeur du laboratoire de recherches en AI du MIT[30] : « *This may upset some of my students at MIT, but one of my concerns is that it's been a predominately male gang of kids, mostly white, who are building the core computer science around AI (…)* ».

***8.*** **Vers un contrôle des systèmes intelligents utilisés par les pouvoirs publics** : Ainsi, on comprend la crainte exprimée récemment par la Commission européenne[31] : *« On ne saurait en effet considérer qu'un algorithme (entendu au sens large comme le système socio-technique dont il fait partie) puisse être « neutre », dans la mesure où il incorpore inévitablement des partis pris –que ceux-ci soient sociaux, politiques, éthiques ou moraux – et répond le plus souvent à des finalités qui incluent une dimension commerciale pour son auteur. »*. C'est pourquoi à la suite des travaux menés par le High Level Group of Experts dont les résultats ont été remis à la Commission européenne[32], nous plaidons, en particulier dans le domaine de l'utilisation d'algorithmes par les pouvoirs publics et singulièrement dans le domaine policier et judiciaire pour la création

---

[28] La France n'a pas suivi l'exemple d'autres pays qui comme la Belgique, ont souhaité soustraire à l'autorité de contrôle 'généraliste', la compétence de surveillance des traitements policiers.

[29] Cf. à cet égard, les considérants identiques n° 20 du RGPD et 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**[29]*, *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,* le contrôle des traitements peut être exercé par une autorité spécifique au sein de l'appareil judiciaire

[30] MIT Media Lab People. ≪ Joi Ito ≫, (pas de date connue), Media.mit.edu (blogue), en ligne : Https://www.media.mit.edu/ <https://www.media.mit.edu/people/joi/overview/>. et MIT Media Lab people, en ligne : Https://www.media.mit.edu/<https://www.media.mit.edu/people/.

[31] *CE, Communication de la Commission au Parlement européen, au Conseil européen, au Conseil, au Comité économique et social européen et au Comité des régions : L'intelligence artificielle pour l'Europe, COM (2018), 237.*

[32] High Level Group of Experts on AI, *Ethics Guidelines for trustworthy AI systems*, décembre 2018, publié par la Commission après commentaires le 9 avril 2019, disponible sur le site: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

d'une « **Autorité nationale pluridisciplinaire indépendante d'évaluation des risques liés à l'intelligence artificielle et en particulier aux traitements de profilage utilisant des procédés d'apprentissage automatique (*machine learning*)** ». Cette autorité indépendante serait en charge de l'audit, des tests, et de la labellisation des systèmes IA des secteurs privé ou public. L'intervention de cette autorité serait obligatoire en matière de IA utilisés à des activités du secteur public même si ceux-ci sont conçus et opérés par des sous-traitants privés. Sous réserve de ce qui pourrait être décidé par les Etats membres à propos des systèmes à risque élevé, son intervention dépendra au contraire d'une démarche volontaire pour les systèmes opérant dans le secteur privé. Au-delà de ce contrôle *a priori*, il est important de réclamer la transparence du fonctionnement des algorithmes décisionnels ou pré-décisionnels utilisés par l'Etat. Comme l'écrivait dès 1971, G. BRAIBANT[33], *« (il) faudrait imposer à l'autorité publique, chaque fois qu'elle se fonde sur les résultats d'un traitement par l'informatique, de faire connaître les données et les programmes à partir desquels ces résultats ont été obtenus ; ces données et programmes pourront ainsi faire l'objet de discussions susceptibles de remettre en cause leurs résultats. »*. L'article L. 311-3-1 du Code des relations entre le public et l'administration, introduit par la loi n°2016_1321 du 7 octobre 2016 traduit ce vœu de l'auteur *: « Sous réserve de l'application du 2° de l'article L. 311-5[34], une décision individuelle prise sur le fondement d'un traitement algorithmique comporte une mention explicite en informant l'intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l'administration à l'intéressé s'il en fait la demande[35]. »*. Cette transparence, si elle n'est pas due au public en matière d'infractions pénales pour des raisons évidentes de sécurité et les besoins de l'enquête, est au moins due, aux termes de l'enquête, aux avocats, aux organes de contrôle et au juge, toutes personnes qui doivent pouvoir contester les vérités sorties de l'ordinateur.

***9.*** **Les catégories de personnes concernées dans les traitements policiers et judiciaires** - L'autre disposition concerne la nécessité de distinction des catégories de personnes concernées par une infraction pénale. L'article 6 de la Directive oblige les responsables des traitements à '*établir, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que:*

*a) les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale;*

---

[33] G. BRAIBANT, « La protection des droits individuels au regard du développement technologique », *Revue internationale de droit comparé*, 1971, 23, p. 812

[34] Qui prévoit des exceptions, notamment celles nécessaires aux besoins de l'enquête, de la sécurité publique, etc…

[35] Les articles L. 311-1-2 et 1-3 précise ce devoir d'information : « *La mention explicite prévue à l'article L. 311-3-1 indique la finalité poursuivie par le traitement algorithmique. Elle rappelle le droit, garanti par cet article, d'obtenir la communication des règles définissant ce traitement et des principales caractéristiques de sa mise en œuvre, ainsi que les modalités d'exercice de ce droit à communication et de saisine, le cas échéant, de la commission d'accès aux documents administratifs, définies par le présent livre. L'administration communique à la personne faisant l'objet d'une décision individuelle prise sur le fondement d'un traitement algorithmique, à la demande de celle-ci, sous une forme intelligible et sous réserve de ne pas porter atteinte à des secrets protégés par la loi, les informations suivantes : 1° Le degré et le mode de contribution du traitement algorithmique à la prise de décision ; 2° Les données traitées et leurs sources ; 3° Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé ; 4° Les opérations effectuées par le traitement ».*

*b) les personnes reconnues coupables d'une infraction pénale;*

*c) les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale; et*

*d) les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux points a) et b).'*

Sans doute, peut-on regretter qu'une catégorie particulière n'ait pas été reconnue à savoir celle reprenant les personnes désignées par des systèmes d'intelligence artificielle ou de profilage ! A défaut, on les rangera dans la catégorie visée par le, point a) mais il m'apparaitrait important de les en distinguer : la suspicion établie au terme d'un processus mené par les humains doit être distinguée de celle résultant du travail d'un ordinateur si 'intelligent' soit-il !

10. **Quid de la durée de conservation de tels 'profils'** ? - La durée de conservation de telles données et profils est peu définie. La Directive autorise une conservation plus longue que celle autorisée par le RGPD qui exige la non conservation au-delà des nécessités d'accomplissement de la finalité spécifique de la collecte, en l'occurrence ce serait au-delà de la clôture d'une affaire pénale menée à propos d'une infraction précise. Le texte exige certes la fixation de délais maxima de conservation par le responsable[36] (ou le législateur) et la mise à jour des dossiers permettant le nettoyage régulier des données qui ne sont plus pertinentes mais 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 et de la prévention des infractions pénales : «*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». »*[37].

---

[36] Sur ce point, on se référera au Considérant n°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*'

[37] De manière plus nuancée, le Rapport du Conseil de l'Europe de 2002 (*Rapport Sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale (2002)* » (disponible à l'adresse suivante : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae51c ) : « *Les données à caractère personnel servant de base à une décision de justice peuvent être conservées dans des dossiers judiciaires pour la durée nécessaire pour respecter les exigences de la procédure. Quand les données ne sont plus nécessaires pour respecter les exigences de la procédure pour laquelle elles ont été collectées, elles ne devraient être conservées qu'à des fins d'une procédure de révision ou à des fins de recherche historique,*

Ainsi, toute possibilité d'intérêt de conservation de la donnée et du profil à des fins policières fussent-elles éloignées de la raison originaire de leur collecte et pour une autorité différente de la première[38] suffit à prolonger la vie de l'information. 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 de données entre des traitements crées dans le cadre, d'une part, de la lutte anti-terroriste et, d'autre part, de la lutte contre l'immigration clandestine. D'autres questions méritent d'être posées : la réhabilitation entraîne-t-elle suppression des données 'dormantes' relatives à la personne réhabilitée ? Il nous semble que tel devrait être le cas, sous peine de priver la décision de réhabilitation de son sens. En ce qui concerne une décision de grâce, par contre, cette mesure exceptionnelle ne correspond pas à un effacement de l'incrimination ni de la condamnation mais simplement de la suppression de ses effets et donc le maintien des données nous apparaît légitime bien évidemment sous réserve des délais qui doivent être fixés par le responsable du traitement, comme exigé par la Directive.

Ce dernier point sur la conservation des données nous amène à la seconde partie de l'exposé qui traite du stockage et de la diffusion des décisions liées à des infractions pénales.

## II. **Le stockage et la diffusion des décisions liées à des infractions pénales.**

---

*scientifique ou statistique. Leur conservation devrait être accompagnée de garanties appropriées et de mesures de sécurité afin d'éviter leur utilisation à d'autres fins. »*

[38] On note que la Directive considère *a priori* comme compatibles les finalités, la poursuite d'infractions pénales par d'autres autorités policières ou en charge de la prévention ou de la détection d'infractions pénales : ainsi à la limite, la lutte contre l'immigration clandestine n'est pas incompatible avec la lutte contre la fraude sociale. A cet égard, lire l'article 4. 2 de la Directive et le commentaire critique 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 s.. On souligne qu'en 2002, le Conseil de l'Europe, dans son « *Rapport Sur l'incidence des principes de la protection des données sur les données judiciaires en matière pénale y compris dans le cadre de la coopération judiciaire en matière pénale (2002*) » (disponible à l'adresse suivante : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae51c ), concluait de manière beaucoup plus restrictive: « *Si l'on considère que la réutilisation de données à caractère personnel collectées dans le cadre d'une procédure pénale est compatible avec ses finalités initiales, une attention particulière pourrait être prêté lorsque: 1) l'affaire pénale et l'affaire civile dans laquelle les données sont réutilisées sont directement liées ; 2) l'affaire pénale et l'affaire administrative pour lesquelles les données sont réutilisées sont directement liées. Si la finalité pour laquelle les données sont réutilisées n'est pas compatible avec la finalité pour laquelle les données ont été collectées, il est possible d'invoquer les exemptions prévues par l'article 9 de la Convention 108. »*

**11. Un double propos –** Là où le droit connaît le 'pardon' de la prescription et souhaite au-delà d'un certain délai assurer la paix sociale[39] la mémoire de l'ordinateur n'a pas de limite temporelle et l'utilisation des données mémorisées peut poursuivre alors des finalités différentes. Tel est le double souci qu'il nous faut rencontrer ici. Deux questions, même si chacune d'elles renvoie à bien d'autres sous-questions retiennent ici notre attention. La première a trait à la question générale de la conservation des données judiciaires par les autorités publiques et de leur éventuelle anonymisation. Nous aurons l'occasion de noter à cet égard que les précautions prises sur base de la protection des données sont, à notre avis, suffisantes même si nous terminerons en pointant une question, qui à notre avis exigerait une attention du législateur national (Point A). La seconde est plus délicate : les informations relatives à la suspicion ou à des condamnations pénales circulent via les canaux de presse au sens le plus large y compris nos réseaux sociaux. Ces canaux qui relatent la condamnation de telle personnalité ou sa libération faute de preuves, la suspicion voire la rumeur relative à telle personne visent bien évidemment notre presse écrite, télévisée ou présente sur le réseau (la presse électronique) au sens strict mais également de plus en plus largement les sites d'informations présents sur les réseaux sociaux : le blog d'un 'journaliste professionnel' qui attire l'attention sur une descente de police chez un voisin, sur le fait que telle personne bien connue est suspectée de fraude voire condamnée. La diffusion de telles informations est généralement confinée aux lecteurs du journal, aux 'amis' facebookiens ou aux lecteurs, abonnés à un blog. Elle peut s'élargir aux dimensions de la planète lorsque reprise par un moteur de recherche ayant pignon sur toutes les rues du monde, elle est offerte à tous les internautes, gratuitement pour peu qu'ils interrogent le moteur de recherche et fortuitement ou non tombent sur l'information relayée. C'est bien évidemment l'affaire Google rappelée en exergue et, au-delà toute la question de ce qui a souvent été présenté comme le conflit entre liberté d'expression et vie privée ou protection des données (Point B).

## A. La diffusion des décisions de justice relatives aux infractions pénales.

**12. Trois restrictions … une même finalité -** Les restrictions sévères mises par le RGPD visent à éviter la double peine ;: celle qui résulté du prononcé de la sanction par le juge et celle qui s'ajouterait du fait de la publication de la décision que les moteurs de recherche retrouveraient sans difficulté. On distinguera trois dispositions : la première, énoncée par l'article 10 du RGPD, concerne les sévères restrictions mises au traitement des données dites judiciaires, c'est-à-dire relatives aux condamnations et infractions pénales ; la deuxième est la décision prise par nombre d'Etats, suite aux exigences du RGPD, de n'admettre la publication des décisions judiciaires y compris non pénales sous une forme 'anonyme'. Enfin, le principe de proportionnalité, principe de base de tout traitement affirmé par l'article 5 du RGPD oblige à n'utiliser les données à caractère personnel que pour la durée nécessaire à la réalisation des finalités du traitement et sur

[39] « *La prescription est très importante en pratique (…). L'action n'est pas éternelle. Le juge ne peut être saisi longtemps après l'inexécution d'un contrat, la commission d'une infraction ou la naissance d'un acte administratif illégal. La paix sociale ne doit plus être perturbée et l'on considère que les situations sont consolidées.* » (E. JEULAND, *Droit processuel général*, 2. éd, Coll. Domat-droit privé, Paris, Montchrestien, 2012, p. 322 et 323.

cette base, l'article 17 du RGPD reconnaît aux personnes concernées un droit à l'oubli. Ces trois mesures seront analysées successivement.

**13. L'article 10 du RGPD -** La '**donnée judiciaire'** est une donnée sensible, elle est définie par l'article 10 par le RGPD qui reprend sans la modifier celle 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, paragraphe1, 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.'.* L'article 10 institue ainsi à défaut d'un monopole de l'autorité publique sur les données relatives aux condamnations pénales et mesures de sûreté connexes, soit le contrôle de leur traitement par cette dernière[40], soit une autorisation étatique avec '*garanties appropriées'*, notamment lorsque la loi ou le droit d'un état membre prévoit soit que la création et la gestion de la base de données de telles décisions est confiée à des entreprises privées sous-traitantes soit que la loi ou le droit d'un Etat membre confie la création et la gestion de bases de données portant sur des infractions pénales spécifiques, à des organisations chargées par la loi de veiller à prévenir la commission de nouvelles infractions ou l'intérêt de tiers[41]

Curieusement le texte ajoute « ***ET** aux infractions* », cet ajout laisse perplexe dans la mesure où c'est la Directive et non le RGPD qui est compétente en matière de prévention ou de poursuites d'infractions[42]. Nous reviendrons sur ce point dans la mesure où la CJEU semble élargir nettement la portée de la notion et l'étendre, au-delà de décisions à proprement parler, à des suspicions d'infractions (voir *infra*, n° 20). Ainsi, on peut imaginer en ce qui concerne cette seconde catégorie des bases de données 'spécifiques' dûment réglementées et on peut souhaiter que ce soit par la loi et après un examen soigné de la proportionnalité et de la sécurité de tels traitements. Deux exemples : pour des raisons de protection des consommateurs, la Banque de France tient depuis des années un registre des interdits de chèque ; demain, les noms des auteurs condamnés de message raciste sur Internet pourraient faire l'objet d'une liste qui facilite leur surveillance par les plateformes de communication et on peut imaginer que le nom des personnes condamnées pour pédophilie puisse circuler dans les écoles et œuvres pour la jeunesse. Encore faudra-t-il assortir ces réglementations de '*garanties*

[40] Ainsi, en cas de sous-traitance par le Ministère de la Justice à une société privée, spécialisée en bases de données. Le contrôle exigera la rédaction d'un contrat de sous-traitance qui apporte les garanties de sécurité souhaitables.

[41] Par exemple, les banques nationales peuvent se voir confier le soin de tenir un répertoire des personnes coupables de faillites frauduleuses ou d'escroquerie de manière consultable par les organismes financiers voire les entreprises de crédit afin de prévenir l'octroi à ces personnes de nouveaux crédits ou le démarrage de nouvelles activités commerciales pendant un laps de temps déterminé. A noter également, que dans le cadre d'une activité normale, les bailleurs sociaux peuvent être amenés à collecter des données relatives à des infractions, condamnations ou mesures de sûreté. Ils doivent, en effet, garantir la jouissance paisible des logements, ce qui les conduit à assurer la tranquillité et la sécurité des résidents et de leurs personnels

[42] Sur ce point, lire notre contribution, Les tribunaux à l'heure du numérique et … des législations de protection des données: de quelques zones d'incertitude, in « LE TRIBUNAL DE L'UNION EUROPÉENNE À L'ÈRE DU NUMÉRIQUE », Actes du COLLOQUE ORGANISÉ À L'OCCASION DU 30ÈME ANNIVERSAIRE DE L'INSTALLATION DU TRIBUNAL DE L'UNION EUROPÉENNE

*appropriées'* comme les contrôles d'accès à la base de données, l'engagement de confidentialité des destinataires autorisés, les limites de conservation des données, etc.

On note que la définition s'entend des seules décisions (condamnations) juridictionnelles et laisse dans l'ombre les données relatives aux suspicions, aux simples accusations entretenues par la rumeur publique ou mises en cause par l'un ou l'autre journaliste. Toutes ces données liées à la commission supposée ou non d'infractions pénales ne sont pas comprises dans le concept de « donnée judiciaire » et on peut le concevoir facilement eu égard au régime lié de monopole de traitement lié à ce concept. On sera d'autant plus surpris par l'extension donnée récemment à la notion par la décision de la CJUE, le 24 septembre de cette année. Nous reviendrons sur ce point (*infra* n° 20)

14. **L'anonymisation' des décisions –** Au-delà des précautions offertes par l'article 10 relatives aux seules décisions relatives aux condamnations pénales et autres mesures de sûreté, la volonté de nombre d'Etats est d'aller plus loin encore en prévenant tout risque d'utilisation des données à caractère personnel contenues dans les décisions qu'elles soient judiciaires ou administratives. La solution est l'anonymisation des décisions[43] ou plutôt leur pseudonymisation[44] voire leur 'occultation', pour reprendre l'expression récemment retenue par l'article 19 du projet de loi française de programmation et de réforme de la Justice 2018- 2024[45]. L'anonymat lors de la publication des jugements est dans tous nos pays un débat délicat. En France, le rapport CADIET[46] analyse les différentes options. Le débat renvoie à de nombreuses questions. S'agit-il d'anonymisation, de pseudonymisation ou d'occultation, terme choisi en France ? Ne faut-il pas procéder à une analyse du risque de ré-identification ? 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

[43] Voilà ce que le rapport à la Chambre des représentants de la récente proposition de loi belge modifiant le Code judiciaire en ce qui concerne la publication des jugements et des arrêts (DOC 54 3489/003, 15 février 2019) notait : « *Les auteurs proposent que les jugements et arrêts soient enregistrés dans une banque de données électronique accessible au public. La mise en service de cette banque de données électronique doit aller de pair avec l'anonymisation des jugements et arrêts, certainement en matière pénale. La proposition de loi ajoute le fondement légal à cet effet dans l'article 782bis du Code judiciaire lequel permet de parachever la mise en œuvre et la concrétisation de cette mesurer par arrêté royal.* »

[44] Comme défini par l'article 4. 1 5) du RGPD : *«pseudonymisation», le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;*

[45] 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.* ». (B. MATTIS et H. RUGGIERI, « L'*open data* des décisions de justice en France
Les enjeux de la mise en œuvre, in le Juge et l'algorithme, Cahiers du CRIDS, 2019, p. 195 et s.)

[46] L. CADIET, « L'open data des décisions de justice - Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice », in *La documentation française,* Paris, janvier 2018.

compte bancaire ?)[47] et à propos de qui (parties au procès, autres personnes citées par le jugement, avocats, magistrats) ? Comment y procéder ?[48]

15. **Le droit à l'oubli -** L'article 16.2 de la Directive consacre de manière très limitée le droit à l'effacement si du moins on compare son libellé à celui de l'article 17.1 du RGPD Ce dernier ouvre à la personne concernée ce droit dans nombre d'hypothèses : retrait du consentement, disparition de la pertinence de la donnée au regard de la finalité, traitement illicite, obligation légale, opposition en raison de la prépondérance de l'intérêt de la personne concernée, … Quant à lui, l'article 16.2 de la Directive[49] limite – et on le conçoit - ce droit à l'effacement, premièrement, lorsque le responsable traite des données de manière illicite, c'est-à-dire en contradiction avec les principes relatifs au traitement dc données à caractère personnel énumérés à l'article 4 ; en deuxième lieu si le traitement sort des compétences du responsable ; en troisième lieu si les données concernent des données dites sensibles ; en quatrième lieu, lorsque « *les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable de traitement* ». C'est ce dernier cas qui, me semble-t-il, mériterait d'être mis en œuvre. Il est intéressant, à cet égard, de rappeler que dans les lois dites de première génération figurait l'interdiction de maintenir au-delà d'une certaine durée certains types de condamnation pénales de manière à permettre à la personne le **repentir** et de ne pas être à vie poursuivie par un péché de jeunesse : ainsi, l'émission d'un chèque sans provision, la condamnation pour fausse déclaration à l'assurance, …. Sans cette intervention législative, il est fort à craindre que le responsable du traitement, la banque, la compagnie d'assurance, ne maintienne une donnée certes ancienne mais dont la non pertinence est d'autant plus contestable à l'heure où on réclame de ces responsables : '*Know your customer'*.

### B. Stockage et diffusion « journalistiques » des informations concernant des infractions pénales.

16. **Retour sur l'affaire Google –** Le point A témoigne de la volonté des autorités publiques de maintenir, nonobstant la puissance des ordinateurs et de leurs logiciels, une réglementation telle qu'elle garantit au justiciable condamné une certaine protection mais cette protection s'avère bien illusoire lorsqu'on constate que les interdictions et protections légales se trouvent contournées par l'activité de certaines entreprises privées qui, au nom de la liberté d'expression, mettent une information parfois subjectivement

---

[47] L'article33 de la loi de programmation de la réforme du judiciaire stipule : « *Par dérogation au premier alinéa, les noms et prénoms des personnes physiques mentionnées dans le jugement, lorsqu'elles sont parties ou tiers sont occultés préalablement à la mise à disposition du public. Lorsque sa divulgation est de nature à porter atteinte à la sécurité ou au respect de ces personnes ou de leur entourage, est également occulté tout élément permettant d'identifier les parties, les tiers et les magistrats et les membres du greffe*. »,

[48] 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 *Le juge et l'algorithme*, Cahiers du CRIDS, 2019, p. 195 et s. ; B. DOCQUIR, « Quelques observations complémentaires sur la publication des décisions », *J .T.*, 2019, p. 449 et s.

[49] Article 16. 2 : « *Les États membres exigent que le responsable du traitement efface dans les meilleurs délais les données à caractère personnel et accordent à la personne concernée le droit d'obtenir du responsable du traitement l'effacement dans les meilleurs délais de données à caractère personnel la concernant lorsque le traitement constitue une violation des dispositions adoptées en vertu de l'article 4, 8 ou 10 ou lorsque les données à caractère personnel doivent être effacées pour respecter une obligation légale à laquelle est soumis le responsable du traitement*. »

biaisée par l'interprétation du 'journaliste', souvent incomplète et, faut-il ajouter souvent sans attendre le verdict final au mépris du respect que l'on doit à la présomption d'innocence. On note en outre que la découverte de cette information prise alors comme argent comptant peut-être fortuite au détour de la frappe d'un mot-clé et s'opère en dehors du contexte bien balisé des bases de données juridiques. Bref à quoi sert-il de multiplier les freins à l'accès aux informations nominatives dans le cadre de la publication officielle des décisions pénales si d'autres canaux bien moins fiables mais aussi bien plus puissants permettent de contourner une telle interdiction. Certes on nous dira avec raison que les journaux ne s'intéressent qu'à peu d'affaires mais même si tel est le cas, la question des limites de la publication au nom de la liberté d'expression mérite d'être posée.

La décision Google mais également des décisions plus récentes de la Cour de Justice européenne ou de la Cour de Strasbourg ont été amenées à mieux circonscrire les termes du débat entre la protection des données, d'une part et de la liberté d'expression d'autre part[50]. Avant d'en donner le bref aperçu de leurs décisions, il importe de rappeler les dispositions du RGPD qui encadrent ce débat.

**17. Les articles 17 et 85 du RGPD -** Le premier paragraphe de l'article 17 énonce : « *La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivant s'applique …* ». Nous ne détaillerons pas les différents motifs applicables. Il suffit de noter que les diverses hypothèses se réfèrent tous à des traitements qui soit sont illicites (notamment, obligation légale d'effacement, collecte de données dans le cadre de services à des « enfants »), soit le deviendraient si le responsable du traitement ne répondait pas à la demande de la personne concernée (exercice du droit d'opposition ou de retrait du consentement, non proportionnalité désormais de la donnée par rapport aux nécessités de la finalité). A ce droit à l'oubli ou plutôt au déférencement[51], le responsable peut opposer suivant le §3 de l'article 17, en particulier lorsque le traitement est « *nécessaire à l'exercice du droit à la liberté d'expression et d'information* ». On note que l'exception du § 3 de l'article 17 ne se réfère plus aux seules activités journalistiques, comme le faisait l'article 9 de la Directive 95/46[52] mais plus largement à l'exercice de la liberté d'expression et d'information. Le considérant n° 153 du RGPD rappelle, à l'instar de la jurisprudence

[50] Le considérant 64 parle de 'pondération équilibrée' à opérer entre ces deux droits fondamentaux. Sur cet équilibre, lire en particulier, Q. VAN ENIS, « La conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel, in *Le règlement général sur la protection des données,* Cahiers du CRIDS, n° 44, p. 763 – 797. N. MALLET-POUJOL, « Les traitements de données personnelles aux fins de journalisme », in *Les nouvelles frontières de la vie privée, Legicom,* n° 43, 2009/2, p. 65 et s. ; T. LEONARD et Y. POULLET,

[51] L'utilisation du terme 'déférencement' est préférable à celui d'oubli qui implique une disparition définitive de la donnée. Dans bien des cas, le responsable devra conserver une trace de la donnée effacée, ne serait-ce que pour prouver qu'il a honoré la demande (par exemple en cas de retrait du consentement) ou pour donner suite à sa demande (je ne vous enverrai plus de publicité ou conformément au § 2 de l'article, le devoir d'informer les tiers auxquels communication de la donnée a été faite de l'exercice par la personne concernée.

[52] *« Les États membres prévoient, pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations au présent chapitre, au chapitre IV et au chapitre VI dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression*.»

européenne en la matière, que les notions liées à la liberté d'expression, et notamment la notion de journalisme, doivent être interprétées largement et ce, « *pour tenir compte de l'importance du droit à la liberté d'expression dans toute société démocratique* ». Ainsi, si l'activité de Google ne peut prétendre relever de l'activité journalistique, il est difficile de nier que son activité, en particulier mais pas uniquement, de moteur de recherche contribue amplement – et c'est peu dire - à la possibilité pour les internautes de s'informer. On souligne par contre que le texte exige que le traitement doit être *nécessaire* à cet exercice. Comment les juges luxembourgeois mais également strasbourgeois ont-ils interprétés l'exception du RGPD ?

Avant d'analyser l'interprétation jurisprudentielle, un mot sur le contenu de l'article 85 : « 1. *Les États membres concilient, par la loi, le droit à la protection des données à caractère personnel au titre du présent règlement et le droit à la liberté d'expression et d'information, y compris le traitement à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire.* 2. *Dans le cadre du traitement réalisé à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, les États membres prévoient des exemptions ou des dérogations au chapitre II (principes), au chapitre III (droits de la personne concernée), au chapitre IV (responsable du traitement et sous-traitant), au chapitre V (transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales), au chapitre VI (autorités de contrôle indépendantes), au chapitre VII (coopération et cohérence) et au chapitre IX (situations particulières de traitement) si celles-ci sont nécessaires pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information.* ». On souligne que le § 2 de cet article semble réserver aux seules activités à des fins journalistiques ou d'expression universitaire, artistique ou littéraire les possibilités pour les Etats membres d'utiliser les exceptions mentionnées alors que le §1 élargissent le devoir de conciliation imposé aux Etats plus largement. Faut-il y voir une erreur du législateur européen ou considère-t-on que désormais tout internaute qui s'exprime sur la toile vis-à-vis d'un public à composition indéterminée sur un sujet d'intérêt général est désormais à considérer comme un journaliste[53] ? Quoiqu'il en soit et sans entrer dans toutes les controverses doctrinales et jurisprudentielles à ce sujet, la question du droit à l'oubli ou au déférencement impose ce devoir d'équilibre sinon au législateur du moins au juge. Or que disent les juges ? Il est intéressant de distinguer à cet égard, les arrêts SATAMEDIA qui abordent la

[53] C'est l'opinion que certains auteurs de doctrine défendent. Ainsi, avec force, J. ENGLEBERT (« La liberté d'expression à l'heure d'Internet » in Cahier du CRIDS, n° 49, à paraître) : « *Il faut en effet inlassablement rappeler que les journalistes n'ont pas le monopole de l'expression d'intérêt général. Ou pour le dire autrement, que le journalisme n'est pas une profession mais une fonction, qui peut – ne déplaise à certains[53] – être endossée par n'importe qui. C'est-à-dire par chaque citoyen. C'est ce qu'a rappelé la Cour constitutionnelle lorsqu'elle a purement et simplement effacé toute référence au « journaliste » de la loi sur la protection du secret des sources journalistiques.* ». On note la même évolution dans la jurisprudence européenne. A cet égard, l'arrât récent du 12 avril 2019 en cause BUYVITS (CJUE, 14 février 2019, Buivids v. DVI, C-345/17), que T. LEONARD et moi-même résumons comme suit : '*Elle (La Cour) y confirme sa jurisprudence antérieure selon laquelle les exemptions prévues par la Directive s'appliquaient non seulement aux entreprises de média, à la presse au sens strict du terme mais aussi à toute personne exerçant des activités de journalisme (§52). Elle rappelle aussi que les « activités de journalisme » sont celles qui ont pour finalité « la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit » (§53), peu importe donc le moyen de communication utilisé (papier, ondes hertziennes ou électronique) et indépendamment d'un but lucratif (§59). Elle précise en outre qu'en l'espèce, le fait que Mr Buivids ne soit pas un journaliste de profession n'empêchait pas qu'une telle finalité puisse être retenue (§56). »*

question à partir de la liberté d'expression et le journalisme et ceux GOOGLE qui réfléchissent à partir des prescrits de protection des données, pour constater qu'in fine la solution est la même et tourne autour de considérations portant sur l'intérêt général

18. **L'affaire SATAMEDIA et la conciliation des deux libertés autour de la notion d'intérêt général –** L'affaire SATAMEDIA[54] qui concernait la « vente » via SMS de données fiscales sur une vaste population de citoyens finlandais a permis aux cours tant de Strasbourg que de Luxembourg de contribuer à définir ce qu'il faut entendre par exercice de la liberté d'expression à des fins journalistiques. En l'occurrence, un éditeur proposait au public de connaître la situation fiscale d'autres citoyens et argumentait, face aux objections de protection de la vie privée, que s'agissant de données rendues publiques suivant la loi finlandaise d'accès aux documents publics, il ne faisait que participer à l'information citoyenne. Dans cette affaire, la Cour luxembourgeoise[55] était saisie d'une question préjudicielle : peut-on parler de journalisme dans le cas de cet éditeur ? Même si elle laisse une possibilité de distinguer l'expression journalistique comme forme particulière de liberté d'expression, la Cour de Luxembourg note que des activités « *peuvent être qualifiées d''activités de journalisme' » de nature à faire entrer en jeu le régime dérogatoire de la directive (en l'espèce l'article 9 de celle-ci), « si elles ont pour finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que soi*t » sans faire aucunement référence à la mission qui incombe à la presse d'informer le public sur toute question d'intérêt général. Ainsi, la Cour juge que les dérogations et exemptions doivent s'appliquer « non seulement aux entreprises de média, mais également à toute personne exerçant une activité de journalisme », sans tenir compte du média utilisé ni de la poursuite d'un but lucratif.

Saisie à son tour quelques années plus tard cette fois sur l'équilibre entre les libertés, la Cour strasbourgeoise[56] affirme que les activités de cette dernière ne pouvaient être considérées comme exercées aux seules fins de journalisme, dès lors que la diffusion telle qu'organisée par ces sociétés n'avaient pas pour finalité la participation à un débat d'intérêt général mais plutôt la satisfaction à des besoins de sensationnalisme et de voyeurisme du public et à l'intérêt purement économique de ces sociétés : « *l'existence d'un intérêt général à ce que de grandes quantités de données fiscales soient accessibles et à ce que la collecte de données soit autorisée ne signifie pas nécessairement ou automatiquement qu'il existe également un intérêt général à diffuser en masse pareilles données brutes, telles quelles, sans aucun apport analytique* » [57]. Que tirer de toutes ces considérations des deux Cours à propos de cette affaire SATAMEDIA, le journalisme est une activité qui peut poursuivre des finalités lucratives et qui déborde les seuls organismes de presse soumis pour leurs activités journalistiques à des obligations déontologiques. La liberté d'expression que promeut le journalisme ne l'emportera sur les exigences de protection des données que si l'activité poursuivie par ces 'journalistes'

---

44 Sur la saga Satamedia et les diverses décisions judiciaires à son propos, .Q. Van Enis, « Le droit de recevoir des informations ou des idées par le biais de l'internet, parent pauvre de la liberté d'expression dans l'ordre juridique européen ? », *JEDH*, 2015/2, pp. 178-179,

[55] C.J.U.E. (GC), 16 décembre 2008, arrêt *Tietosuojavaltuutettu contre Satakunnan Markkinaporssi Oy et Satamedia Oy*, C-73/07.

[56] Cour eur. D.H. (GC), arrêt du 27 juin 2017. Pour des commentaires de cet arrêt, D. Voorhoof, « No journalism exception for massive exposure of personal taxation data », *Strasbourg Observers*, 5 juillet 2017 : https://strasbourgobservers.com/2017/07/05//no-journalism-exception-for-massive-exposure-of-personal-taxation-data/.

[57] Arrêt précité, § 175

est nécessaire à l'accomplissement de la « finalité journalistique », c'est à dire poursuit un intérêt général, à savoir promouvoir le débat public sur des sujets d'intérêts généraux[58]. Pour bénéficier de la dérogation prévue à l'article 17 § 3, la poursuite de cet intérêt général devra être invoquée outre, le cas échéant, celle de l'intérêt économique du journaliste (liberté d'entreprendre) et la considération de ces intérêts ainsi poursuivis devra l'emporter sur l'intérêt de la personne concernée au respect de sa vie privée et de la protection de ses données. Cette réflexion laisse entendre que le débat ne doit pas être posé en termes d'opposition des deux libertés (droit à la liberté d'expression versus droit à la protection des données) mais plutôt en termes de contribution de ces deux libertés à l'intérêt général. La protection des données n'est pas une liberté robinsonienne absolue[59] attachée à la défense des seuls intérêts purement individualiste, elle entend permettre à l'individu de jouer pleinement son rôle à l'intérieur de la société et, en ce sens, trouve dans l'intérêt général les limites à une revendication purement individualiste.

19. **L' arrêt Google Spain** – Le premier arrêt : le fameux Google Spain[60] a précédé l'adoption du RGPD et concerne donc l'ancienne Directive 95/47, en particulier le droit d'opposition et le droit de suppression. Diverses leçons peuvent être tirées de cet arrêt qui a fait date et a fortement influencé le contenu du RGPD pas seulement sur le point que nous analysons ici. La première leçons est la reconnaissance par la Cour de l'intérêt du rôle joué par Google dans la diffusion d'informations : « *En outre, il est constant que cette activité des moteurs de recherche joue un rôle décisif dans la diffusion globale desdites données en ce qu'elle rend celles-ci accessibles à tout internaute effectuant une recherche à partir du nom de la personne concernée, y compris aux internautes qui, autrement, n'auraient pas trouvé la page web sur laquelle ces mêmes données sont publiées. De plus, l'organisation et l'agrégation des informations publiées sur Internet effectuées par les moteurs de recherche dans le but de faciliter à leurs utilisateurs l'accès à celles-ci peut conduire, lorsque la recherche de ces derniers est effectuée à partir du nom d'une personne physique, à ce que ceux-ci obtiennent par la liste de résultats un aperçu structuré des informations relatives à cette personne trouvables sur Internet leur permettant d'établir un profil plus ou moins détaillé de la personne concernée,* Dans le même temps, elle note les risques supplémentaires encourus par la personne concernée du fait de l'agrégation des données permise par le moteur de recherche. Ces risques ne sont d'ailleurs pas qu'individuels mais concernent nombre de citoyens. Il est intéressant de noter l'insistance que les juges mettent sur ce point. Le risque est collectif et non simplement individuel et doit être pris en considération en tant

[58] Cette position est proche de celle développée par l'avocat général KOKOTT dans ces conclusions présentées le 8 mai 2008 à propos de l'affaire SATAMEDIA alors portée devant la CJUE : « le traitement de données à caractère personnel est (...) effectué à des fins de journalisme lorsqu'il vise la communication d'informations et d'idées sur des questions d'intérêt public ». Notre propos est simplement de ne pas confondre les activités journalistiques ou le journalisme qui peuvent être développées dans des perspectives de pur intérêt économique, comme dans l'affaire SATAMEDIA et la finalité journalistique qui s'entend des seules activités qui visent à promouvoir le débat sur des questions d'intérêt public. Sur cette finalité journalistique qui expliquent le régime dérogatoire du journaliste, lire V. ENGLEBERT, article cité.

[59] Voir le Considérant 4 du RGPD : *« **Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu ; il doit être considéré par rapport à sa fonction dans la société** et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité*. » (nous soulignons)

[60] CJUE, 13 mai 2014, Google Spain et Google Inc. c. Agenzia Espanola de Proteccio de Datos, C-131/12. A propos de cette affaire, lire entre autres, E. CRUYSMANS, « La protection de la réputation en ligne », in *L'Europe des droits de l'Homme à l'heure d'Internet*, in Q. VAN ENIS et C. de TERWANGNE (eds.), Bruylant, Bruxelles, 2019, p. 401 et s.

que tel. On voit poindre ici à côté d'une défense de l'intérêt individuel de la personne de Mr COSTEJA, celle de l'intérêt général.

La deuxième leçon concerne la recherche de l'équilibre d'intérêts entre ceux économiques de l'exploitant du moteur de recherche voire des tiers et le besoin de protection des données de la personne concernée : « *Au vu de la gravité potentielle de cette ingérence (*que représente le fonctionnement du moteur de recherche de Google (NdlA)), *force est de constater que celle-ci ne saurait être justifiée par le seul intérêt économique de l'exploitant d'un tel moteur dans ce traitement. Cependant, dans la mesure où la suppression de liens de la liste de résultats pourrait, en fonction de l'information en cause, avoir des répercussions sur l'intérêt légitime des internautes potentiellement intéressés à avoir accès à celle-ci, il y a lieu de rechercher, dans des situations telles que celles en cause au principal, un juste équilibre notamment entre cet intérêt et les droits fondamentaux de cette personne au titre des articles 7 et 8 de la Charte. Si, certes, les droits de la personne concernée protégés par ces articles prévalent également, en règle générale, sur ledit intérêt des internautes, cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique.* ».

Cette référence à l'intérêt du public à une information d'intérêt général[61] pourrait donc, c'est la troisième leçon, justifier d'une exception en faveur du maintien de l'information. En d'autres termes, c'est l'apport à un débat sur un sujet d'intérêt général, ce que l'arrêt SATAMEDIA de la CEDH appelle l''exercice de la liberté d'expression à des fins journalistiques, qui pourrait justifier le droit à l'oubli. Cependant, le bénéfice de cette exception n'est pas applicable, quatrième leçon à un moteur de recherche, mais bien à l'éditeur de la page web originaire soit le journal La Vanguardia : *« En outre, le traitement par l'éditeur d'une page web, consistant dans la publication d'informations relatives à une personne physique, peut, le cas échéant, être effectué «aux seules fins de journalisme» et ainsi bénéficier, en vertu de l'article 9 de la directive 95/46, de dérogations aux exigences établies par celle-ci, tandis que tel n'apparaît pas être le cas s'agissant du traitement effectué par l'exploitant d'un moteur de recherche…. l'exploitant d'un moteur de recherche est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne, également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite. »*

**20. Les deux arrêts Google du 24 septembre 2019 -** Le Conseil d'Etat français a entendu, par des questions préjudicielles[62] toujours à propos du moteur de recherches GOOGLE, faire approfondir cette première décision : la première affaire porte sur l'étendue territoriale du déférencement lorsque celui-ci se fonde sur les exceptions rendant

[61] C'est par un attendu sur ce point que se termine l'arrêt : « *Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question. »*

[62] Demande préjudicielle du Conseil d'Etat français en date du 20 août 2017

envisageable le traitement de données sensibles (en l'occurrence précisément des suspicions d'infractions pénales et des condamnations pénales) ou sur la dérogation prévue à des fins de journalisme (Arrêt 24 septembre 2019, dans l'affaire C-136/17) ; la seconde sur le fait que le déférencement doit ou non s'appliquer sur l'ensemble des noms de domaine (Arrêt 24 septembre 2019 - Dans l'affaire C-507/17). La première nous intéressera particulièrement. En l'occurrence, la personne concernée demandait le déréférencement de liens qui mènent vers des articles, principalement de presse, relatifs à l'information judiciaire ouverte au mois de juin 1995 sur le financement du parti républicain (PR). Mis en examen, la procédure le concernant a été clôturée par une ordonnance de non-lieu le 26 février 2010. La plupart des liens litigieux mène vers des articles qui sont contemporains de l'ouverture de l'instruction et ne font en conséquence pas état de l'issue de la procédure.

21. **Le premier arrêt – de nouvelles obligations pour les opérateurs de moteur de recherche -** Les juges luxembourgeois interprètent comme suit l'article 17 § 3 : « *La circonstance que l'article 17, paragraphe 3, sous a), du règlement 2016/679 prévoit désormais expressément que le droit à l'effacement de la personne concernée est exclu lorsque le traitement est nécessaire à l'exercice du droit relatif, notamment, à la liberté d'information, garantie par l'article 11 de la Charte,* ***constitue une expression du fait que le droit à la protection des données à caractère personnel n'est pas un droit absolu, mais doit, ainsi que le souligne le considérant 4 de ce règlement, être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité*** *[voir, également, arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 48, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 136]*. ». Cette interprétation conduit à affirmer l'obligation de *« l'exploitant d'un moteur de recherche, lorsqu'il est saisi d'une demande de déréférencement, doit vérifier, au titre des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de la directive 95/46 ou à l'article 9, paragraphe 2, sous g), du règlement 2016/679 et dans le respect des conditions prévues à ces dispositions, si l'inclusion du lien vers la page web en question dans la liste affichée à la suite d'une recherche effectuée à partir du nom de la personne concernée est nécessaire à l'exercice du droit à la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche, protégée par l'article 11 de la Charte* »[63].

La prévalence des droits de la personne concernée est d'autant plus nécessaire que les données en cause sont des données sensibles au regard du RGPD. A cet égard, on relève l'extension donnée à la notion de données judiciaires par les juges[64] : « *les informations concernant une procédure judiciaire menée contre une personne physique, telles que celles relatant sa mise en examen ou le procès, et, le cas échéant, la condamnation qui en a résulté, constituent des données relatives aux « infractions » et aux*

[63] Les juges ajoutent que la pondération doit aller dans le sens de la protection des personnes concernées sauf à estimer à « *l'inclusion de ce lien dans la liste de résultats, qui est affichée à la suite d'une recherche effectuée à partir du nom de cette personne, s'avère strictement nécessaire pour protéger la liberté d'information des internautes potentiellement intéressés à avoir accès à cette page web au moyen d'une telle recherche, consacrée à l'article 11 de la Charte*. »

[64] Voir sur cette extension étonnante non sur le fond mais au vu les domaines respectifs du RGPD et de la Directive, nos remarques supra n° 13

*« condamnations pénales », au sens de l'article 8, paragraphe 5, premier alinéa, de la directive 95/46 et de l'article 10 du règlement 2016/679, et ce indépendamment du fait que, au cours de cette procédure judiciaire, la commission de l'infraction pour laquelle la personne était poursuivie a effectivement été établie ou non. » . Dès lors, le déférencement doit exister portant sur des liens vers des pages web, sur lesquelles figurent de telles informations, lorsque ces informations se rapportent à une étape antérieure de la procédure judiciaire en cause et ne correspondent plus, compte tenu du déroulement de celle-ci, à la situation actuelle.* »[65]

Dernier point : si les juges estiment que les droits de la personne concernée doivent conduire à l'effacement des liens proposés par l'outil de recherche et que pèse sur l'exploitant de l'outil un devoir de vérification et de mise à jour, ils ont soin de rappeler que l'intérêt général fait au contraire un devoir aux éditeurs de base (les journalistes et la presse) de participer à la formation de l'opinion publique tant par la dénonciation de faits même si non encore totalement établis par l'autorité judiciaire que par la mise à disposition d'anciens reportages[66].

En conclusion, les juges retiennent : « *d'une part, les informations relatives à une procédure judiciaire dont une personne physique a été l'objet ainsi que, le cas échéant, celles relatives à la condamnation qui en a découlé constituent des données relatives aux « infractions » et aux « condamnations pénales », au sens de l'article 8, paragraphe 5, de cette directive, et*

*– d'autre part, l'exploitant d'un moteur de recherche est tenu de faire droit à une demande de déréférencement portant sur des liens vers des pages web, sur lesquelles figurent de telles informations, lorsque ces informations se rapportent à une étape antérieure de la procédure judiciaire en cause et ne correspondent plus, compte tenu du déroulement de celle-ci, à la situation actuelle, dans la mesure où il est constaté, dans le cadre de la vérification des motifs d'intérêt public important visés à l'article 8, paragraphe 4, de ladite directive, que, eu égard à l'ensemble des circonstances de l'espèce, les droits fondamentaux de la personne concernée, garantis par les articles 7*

[65] Cette assimilation qui va à l'encontre de l'interprétation restrictive que l'on doit aux exceptions des articles 9 et 10 à la réglementation des données à caractère personnel si elle peut être suivie sur le fond pose cependant un problème quant aux conséquences de cette assimilation, dans la mesure où le RGPD affirme le monopole des autorités publiques en ce qui concerne leur traitement.

[66] Point 76 : « *À cet égard, il convient de relever qu'il ressort de la jurisprudence de la Cour européenne des droits de l'homme que des demandes adressées par les personnes concernées en vue de l'interdiction, en vertu de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, d'une mise à disposition sur Internet, par les différents médias, d'anciens reportages concernant un procès pénal qui avait été dirigé contre ces personnes, appellent un examen du juste équilibre à ménager entre le droit au respect de la vie privée desdites personnes et, notamment, la liberté d'information du public. Dans la recherche de ce juste équilibre, il doit être tenu compte du rôle essentiel que la presse joue dans une société démocratique et qui inclut la rédaction de comptes rendus et de commentaires sur les procédures judiciaires. En outre, à la fonction des médias consistant à communiquer de telles informations et idées s'ajoute le droit, pour le public, d'en recevoir. La Cour européenne des droits de l'homme a reconnu, dans ce contexte, que le public avait un intérêt non seulement à être informé sur un événement d'actualité, mais aussi à pouvoir faire des recherches sur des événements passés, l'étendue de l'intérêt du public quant aux procédures pénales étant toutefois variable et pouvant évoluer au cours du temps en fonction, notamment, des circonstances de l'affaire (Cour EDH, 28 juin 2018, M. L. et W. W. c. Allemagne, CE:ECHR:2018:0628JUD006079810, § 89 et 100 à 102) ».*

*et 8 de la charte des droits fondamentaux de l'Union européenne, prévalent sur ceux des internautes potentiellement intéressés, protégés par l'article 11 de cette charte.* »

**22. La portée territoriale du déférencement -** Le second arrêt met l'accent sur la portée de l'obligation de déférencement que doit opérer un exploitant d'un moteur de recherche opérant dans l'ensemble du monde. A cet égard, les juges soulignent les conceptions différentes que chaque pays européen et *a fortiori* non européen peut avoir de l'équilibre entre liberté d'expression et d'information et protection des données consacré par l'article 11 de la Charte européenne des droits fondamentaux, comme le reconnait l'article 85 au sein de l'espace européen. Dès lors, les juges estiment que**,** lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de l'article 17, il est tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres, et ce, si nécessaire, en combinaison avec des mesures qui, tout en satisfaisant aux exigences légales, permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès aux liens qui font l'objet de cette demande. Ainsi, un tel déréférencement doit, si nécessaire, être accompagné de mesures qui permettent effectivement d'empêcher ou, à tout le moins, de sérieusement décourager les internautes effectuant une recherche sur la base du nom de la personne concernée à partir de l'un des États membres d'avoir, par la liste de résultats affichée à la suite de cette recherche, accès, via une version de ce moteur « hors UE », aux liens qui font l'objet de la demande de déréférencement. La juridiction nationale ou, pour être plus précis, l'autorité nationale de contrôle devra vérifier que les mesures mises en place par Google Inc. dans le cas tranché demain d'autres plateformes comme par exemple You Tube, satisfont à ces exigences.

**23. Une certaine perplexité –** Arrivé au terme de ce second chapitre, j'avoue une certaine perplexité quant aux conséquences pratiques de la décision. Sans doute très généreuse en faveur de la protection des données judiciaires, la décision du 24 septembre semble bien introduire l'idée du pardon numérique et empêcher les diffusions en tout cas massives tantôt erronées, tantôt non contextualisées, tantôt non mises à jour des suspicions, incriminations et condamnations pénales. La liberté d'expression ne légitime pas la conservation indéfinie des liens vers les sites d'information journalistiques ou non diffusant des données judiciaires au sens le plus large que lui donne désormais la CJUE. Ce n'est que dans la mesure où la diffusion participe « aux fins journalistiques », à savoir nourrit le débat public sur des questions d'intérêt général que leur présence sur les moteurs de recherche doit être admise. Au-delà, il est fait obligation aux moteurs de recherche de veiller à 'effacer les données' en tenant compte du fait que les exigences de la liberté d'information et d'expression peuvent se comprendre différemment suivant les pays. Bref, voilà l'exploitant du moteur de recherche dans une position délicate. Lui faudra-t-il à chaque demande devenir 'juge' de cet équilibre des deux libertés ? Doit-il en outre, préventivement, se munir d'un logiciel de préférence d'intelligence artificielle chargé de repérer ces fameuses données judiciaires et de prendre la décision *ad hoc ?* Qui contrôlera la qualité de ce logiciel, l'absence de biais, etc. ? On peut imaginer, comme en matière de lutte contre la désinformation, la création par les exploitants d'une commission plus ou moins indépendante de ' *fast checkers',* chargés d'analyser dans l'urgence les demandes de

déférencement ou, comme en matière de lutte contre les copies illicites[67][68], donner une délégation aux moteurs de recherche pour prévenir les publications de données judiciaires, publications devenues illicites, faute de mises à jour ou désormais objet d'une prescription légale[69]. N'est-ce pas là leur confier là des tâches en principe réservées à l'autorité publique ?

## Conclusions générales

**24. Le numérique un outil à mettre au service de la Justice –** Le titre de cette conclusion constitue un appel plus qu'une condamnation du numérique ou, à l'inverse, une confiance en celui-ci.

La première partie a montré combien le numérique pouvait, sous prétexte de l'efficacité qu'il apporte à la gestion des enquêtes, à la détection des suspects voire des coupables voire à la décision désormais 'robotisée, devenir l'instrument d'une justice qui ne soit plus humaine et qui remplace l'application de la loi par un algorithme décisionnel. S'il ne faut pas lier l'apport incontestable de l'ordinateur à la Justice, il importe de rappeler que la Justice est d'abord œuvre d'homme pour des hommes et qu'en définitive, le dernier mot doit rester à l'humain. Mettre l'ordinateur au service de l'humain, c'est exiger que son fonctionnement soit transparent, que les balises qu'impose les principes du '*fair trial'* et les exigences de protection des données à caractère personnel soient pleinement respectés.

La seconde partie témoigne des dangers de la mémoire et de la puissance communicationnelle des ordinateurs qui mettent à mal le 'pardon' qu'exige le droit. Nous avons montré combien la réglementation de la protection des données a encadré la donnée judiciaire mais, au-delà plus récemment, combien la jurisprudence a entendu rappeler le service d'intérêt général que poursuit la liberté d'expression dans le débat démocratique mais dans le même temps a reconnu les limites qu'impose à cette liberté la protection des données personnelles chaque fois que la diffusion d'une information sensible à grande échelle par les plateformes de communication ou d'information comme Google ne rencontre pas les besoins de cette contribution au débat démocratique. Sur cette base, elle impose aux moteurs de recherche d'utiliser l'outil numérique pour respecter ce délicat équilibre qu'arbitre l'intérêt général.

Ainsi, loin de condamner l'outil numérique et son utilisation, c'est plutôt le mythe de sa

---

[67] Il s'agit de la Directive 'Droit d'auteur et marché unique digital' du 24 mars 2019, qui en son article 17. 7 prescrit : « *La coopération entre les fournisseurs de services de partage de contenus en ligne et les titulaires de droits ne conduit pas à empêcher la mise à disposition d'œuvres ou d'autres objets protégés téléversés par des utilisateurs, qui ne portent pas atteinte au droit d'auteur et aux droits voisins, y compris lorsque ces œuvres ou autres objets protégés sont couverts par une exception ou une limitation.*
*Les États membres veillent à ce que les utilisateurs dans chaque État membre puissent se prévaloir de l'une quelconque des exceptions ou limitations existantes suivantes lors du téléversement et de la mise à disposition de contenus générés par les utilisateurs sur les services de partage de contenus en ligne. »*

[68] Cf. le *Code of Practice on disinformation* signé en octobre 2018 par les plateformes Google, Twitter, Instagram, Microsoft et l'association des entreprises publicitaires à l'instigation de la Commission européenne

[69] Précisément à propos des prescriptions légales, doit-on considérer que l'exploitant serait tenu d'effacer automatiquement les données des condamnations judiciaires au terme de la prescription légale ?

toute-puissance qu'il importe de combattre…. La tâche n'est pas aisée mais elle est cruciale si on souhaite la survie d'un droit et d'une justice humains.