PLAIDOYER VISANT À L'ADOPTION RAPIDE D'UN ACTE UNIFORME OHADA SUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET EXPOSÉ DES MOYENS AUTORISANT LE TRANSFERT DE CES DONNÉES DE L'UNION EUROPÉENNE VERS DES PAYS TIERS

I. Introduction

1. La mondialisation du numérique, l'utilisation de l'Internet, l'utilisation de nouvelles technologies et le besoin de communication et de consommation des services ... sont des occasions donnant lieu à des traitements de données à caractère personnel.

En effet, plus personne n'échappe à la collecte des données personnelles pour des raisons telles qu'évoquées ci-dessus ; nous-mêmes, pour nous rendre à ces assises avons subi la collecte de nos données personnelles à l'aéroport, à un distributeur de banque, dans un supermarché, en passant un coup de fil, etc.

On peut lire dans un rapport intitulé : Surveillance Giants récemment publié par une grande organisation de défenses des droits l'homme « Google et Facebook dominent nos vies modernes ; ils ont accumulé un pouvoir inégalé sur la sphère du numérique en collectant et en monétisant les données personnelles de milliards d'utilisateurs. Leur contrôle insidieux de nos vies numériques sape le fondement même de la vie privée et c'est l'un des défis majeurs de notre époque en termes de droits humains »[1].

Nous partageons le point de vue de Kumi Naidoo, secrétaire général d'Amnisty International, lorsqu'il dit, je cite, « À l'ère numérique, afin de protéger nos valeurs humaines fondamentales – dignité, autonomie et vie privée – il faut une refonte radicale du fonctionnement des géants de la haute technologie et l'essor d'un Internet qui accorde la priorité aux droits humains[2]» .

2. La protection de la vie privée doit également être une priorité pour les États parce qu'ils sont également responsables de traitement pour des fins diverses.

On pense par exemple à l'introduction de la dimension électronique dans le Registre du Commerce et du Crédit Mobilier (RCCM) et ses fichiers connexes institués par les articles 34 et suivants de l'acte uniforme révisé portant sur le droit commercial général, adopté le 15 décembre 2010 à Lomé[3].

Une telle base de données à caractère personnel présente évidemment des dangers pour les commerçants dont les données à caractère personnel sont traitées, dangers auxquelles il devrait être obvié par une législation relative à la protection des données[4].

[1] Amnesty International, "Surveillance giants: how the business model of google and facebook threatens human rights", 21 novembre 2019, [1] https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF
[2] https://www.amnesty.fr/actualites/facebook-et-google-les-geants-de-la-surveillance
[3] http://www.ohada.com/actes-uniformes/940/1296/preambule.html
[4] D. Allechi, « L'informatisation du RCCM et la protection des données à caractère personnel », Village de la justice, 2 mai 2019, https://www.village-justice.com/articles/informatisation-rccm-protection-des-donnees-caractere-personnel,31379.html.

3. Enfin, une telle législation, si elle est reconnue par la Commission européenne comme offrant un niveau de protection adéquat, facilite le transfert de données à caractère personnel encadrées par le RGPD vers ces pays tiers (voy. infra).

4. La Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel – appelée aussi « Convention de Malabo » – a été adoptée à cette fin le 27 juin 2014[5] .

Pour faciliter la mise en œuvre de la Convention, la Commission de l'Union africaine a demandé à l'Internet Society d'élaborer conjointement les Lignes directrices sur la protection de la vie privée et des données à caractère personnel pour l'Afrique[6].

Elle vise, en vertu de son article 8, à ce que chaque État partie mette en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel.

L'échéance des dernières signatures était fixée au 14 mars 2018. Or, force est constater que seuls 14 pays sur les 55 de l'Afrique ont signé cette convention : Bénin, Tchad, Comores, Congo, Ghana, Guinée-Bissau, Mozambique, Mauritanie, Rwanda, Sierra Leone, São Tomé-et-Príncipe, Togo, Tunisie et Zambie.

Et encore, seulement cinq pays – Ghana, Guinée, Ile Maurice, Namibie et Sénégal – l'ont ratifiée pour que celle-ci entre en vigueur sur leur territoire national …

On peut donc craindre que cette convention soit un échec[7].

5. Si l'on examine les législations des États OHADA, tous les États parties ne sont pas dotés d'une telle législation et parmi ceux qui en sont dotés, certaines de leur législation sont obsolètes :

- Le Benin est doté d'une loi 2009-09 du 27 avril 2009 portant protection des données à caractère personnel[8];
- Le Burkina Faso est doté d'une loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel[9];
- Le Cameroun est doté d'une loi 2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité[10];
- Le Congo-Brazzaville a adopté le 30 juillet 2019 une loi portant protection des données à caractère personnel ;
- La Cote d'ivoire est dotée d'une loi 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel[11];
- Le Gabon est doté d'une loi 01-2011 du 25 septembre 2011 relative à la protection des données à caractère personnel[12];
- La Guinée est dotée d'une loi 2016/037 du 28 juillet 2016 relative à la protection des données à caractère personnel[13];
- Le Mali est doté d'une loi 2013-015 du 21 mai 2013 portant protection des données à caractère personnel[14];
- Le Niger est doté d'une loi 2017-28 du 3 mai 2017 relative à la protection des données à caractère personnel[15];
- Le Sénégal est doté d'une loi 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel[16];
- Le Tchad, notre hôte, est doté d'une loi 007/PR/2015 du 10 février 2015 portant protection des données à caractère personnel[17];
- Et enfin, le Togo vient de se doter d'une loi du 23 octobre 2019 relative à la protection des données à caractère personnel.

[5] https://au.int/fr/node/29560
[6] Lignes directrices sur la protection de la vie privée et des données à caractère personnel pour l'Afrique, 9 mai 2018, https://www.internetsociety.org/fr/resources/doc/2018/personal-data-protection-guidelines-for-africa/
[7] C. de Laubier, « L'Afrique se met en ordre de bataille contre la cybermalveillance et la cybercriminalité », 5 août 2018, https://cio-mag.com/lafrique-se-met-en-ordre-de-bataille-contre-la-cybermalveillance-et-la-cybercriminalite/
[8] https://www.afapdp.org/wp-content/uploads/2018/05/Benin-LOI-SUR-PROTECTION-DES-DONNEES-A-CARACTERE-PERSONNEL-2009.pdf
[9] https://www.afapdp.org/wp-content/uploads/2018/05/Burkina-Faso-Loi-portant-protection-des-donnees-a-caractere-personnel-2004.pdf
[10] https://www.unodc.org/res/cld/document/cmr/2010/loi_sur_la_cybersecurite_et_la_cybercriminalite_html/Loi_2010-012_cybersecurite_cybercriminalite.pdf
[11] http://www.artci.ci/index.php/lois/Lois-et-Ordonnances/lois.html
[12] https://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-à-la-protection-des-données-personnelles-du-4-mai-20112.pdf
[13] https://www.afapdp.org/wp-content/uploads/2018/05/Guinee-loi_2016037an_relative_a_la_cybersecurite_et_protection_des_donees.pdf
[14] https://www.afapdp.org/wp-content/uploads/2018/05/Mali-Loi-sur-la-protection-des-donnees-personnelles-du-21-mai-2013.pdf
[15] https://www.afapdp.org/wp-content/uploads/2017/02/Loi-n°2017-28-du-03-mai-2017.pdf
[16] https://www.afapdp.org/wp-content/uploads/2018/05/Senegal-texte-de-loi-2008.pdf
[17] http://www.ansice.td/W3/images/LOI07.pdf

II. Plaidoyer pour l'adoption d'un acte uniforme OHADA sur la protection des données à caractère personnel et à la libre circulation de ces données

6. L'Union européenne s'est dotée d'un nouveau règlement général sur la protection des données à caractère personnel (RGPD)[18] pour deux raisons : une uniformisation de la législation et une prise en compte des nouvelles technologies et des nouveaux risques pour la protection de la vie privée.

En effet, malgré l'inspiration commune de la directive 95/46, les législations européennes étaient trop diverses et cela nuisait à l'efficacité des entreprises européennes et à la libre circulation des données.

Par ailleurs, si en 1995 on se méfiait des États, il devenait urgent d'encadrer également l'activité des GAFA et leurs nouveaux moyens technologiques.

7. Du fait de l'hétérogénéité de législations, parfois obsolètes, de ses États parties et que certains de ceux-ci ne disposent même pas de législation sur la protection des données, nous estimons[19] qu'il est temps pour l'OHADA de se doter d'un acte uniforme relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, à l'instar du RGPD.

Un tel acte pourrait en outre être reconnu comme offrant un niveau de protection adéquat autorisant le transfert de données à caractère personnel de l'Union européenne vers les États parties de l'OHADA (voy. infra).

À défaut, les entreprises africaines seront en outre victimes si pas du protectionnisme de l'Union européenne, de sa stricte protection des données.

III. La stricte protection des données à caractère personnel au sein de l'Union européenne du RGPD

8. En effet, les règles encadrant la vie privée et les traitements de données à caractère personnel en vigueur au sein de l'Union européenne sont considérées internationalement comme étant particulièrement protectrices des citoyens, ou contraignantes pour les entreprises, spécialement non européennes, selon le point de vue.

Bien qu'appliqué avec plus ou moins de vigueur selon les États membres et les différentes autorités nationales de protection des données, le RGPD[20] forme un cadre cohérent à l'intérieur des frontières de l'Union.

Toutefois, les flux internationaux de données sont inhérents au monde globalisé dans lequel les citoyens de l'Union se meuvent, singulièrement depuis l'avènement du Cloud, dont les plus grands acteurs ne se situent pas sur le territoire européen.

L'utilisateur d'Internet ne sait pas toujours si le site web qu'il va visiter et auquel il va fournir des données est établi ou non sur le territoire de l'Espace économique européen (EEE)[21].

[18] Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données), JOUE L 119 du 4 mai 2016, p. 1 ; Rectificatif, JOUE L 127 du 23 mai 2018, p. 2 (2016/679) ; https://eur-lex.europa.eu.
[19] À l'instar d'autres auteurs comme Mouhamadou Lô, auteur d'un livre sur « La protection des données à caractère personnel en Afrique ».
[20] Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement Général sur la Protection des Données), JOUE L 119 du 4 mai 2016, p. 1 ; Rectificatif, JOUE L 127 du 23 mai 2018, p. 2 (2016/679) ; https://eur-lex.europa.eu.
[21] Le RGPD est entré en vigueur, le 20 juillet 2018, en Islande, Norvège et Liechtenstein, https://www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576.

Des données à caractère personnel peuvent donc être traitées dans d'autres pays du globe n'offrant pas un niveau de protection de la vie privée équivalent, voire aucune protection.

La portée des droits conférés par le règlement serait dérisoire si les internautes européens bénéficiaient d'une protection précaire face aux entreprises étrangères qui exercent des activités dans l'EEE.

9. La technologie et la globalisation induisent une multitude de transferts de données transfrontières. Le responsable du traitement, soumis au règlement, peut transférer les données à caractère personnel vers des tiers ou faire appel à des sous-traitants étrangers. Le RGPD autorise ces flux, mais les règles sont différentes lorsque les données sont transférées au sein de ou en dehors de l'Union européenne.

IV. Les transferts de données à des responsables de traitement ou à des sous-traitants établis en-dehors de l'Union européenne

10. Grâce au RGPD, les États membres appliquent le même niveau de protection lors du traitement de données à caractère personnel.

Un transfert **au sein de** l'Union européenne est par conséquent autorisé et régi de la même manière qu'un transfert au sein d'un même État et doit donc respecter les principes généraux de la loi (respect notamment des principes de légitimité, compatibilité de la communication avec le traitement d'origine, information des personnes concernées).

11. Les choses sont différentes si le responsable de traitement souhaite exporter des données à caractère personnel **hors de** l'Union européenne.

L'article 44 du RGPD dispose qu' : « un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis. »

12. Ni la directive antérieure 95/46, ni le règlement ne définissent cette notion de «transfert». Le transfert de données suppose un déplacement effectif de données à l'étranger, quel que soit le support utilisé, dans le but de faire l'objet d'un traitement. Rendre accessible des données sur un serveur informatique à partir de l'étranger ne constituerait par contre pas un transfert selon une frange de la doctrine[22] se basant sur une interprétation de l'arrêt *Lindqvist de* la Cour de Justice[23]. Cette interprétation est toutefois critiquée par une autre partie de la doctrine[24].

En suivant ces derniers auteurs, il convient effectivement de tenir compte du caractère limité de la question préjudicielle ayant amené la Cour de Justice à se prononcer en partie sur la notion de transfert dans l'arrêt Lindqvist. Une manière de réconcilier les positions tout en tenant compte du libellé du RGPD est de considérer que le transfert de données visé par le RGPD suppose, à la fois, un déplacement effectif de donnée et un objectif de traitement dans un pays tiers.

[22] V. notamment l'avis prudent de B. DOCQUIR, *«Le droit de la vie privée»*, Bruxelles, Larcier, 2008, p. 244.
[23] CJCE, 6 novembre 2003, aff. C-101/01, *Lindqvist*.
[24] V. notamment C. DE TERWAGNE (ed.), *«Vie privée et données à caractère personnel»*, Bruxelles, Politiea, 2014, chapitre 4.2/2.

Il est à noter que le transfert de données constitue en tant que tel un traitement de données et qu'il doit donc respecter, outre les règles encadrant le transfert, l'ensemble des règles afférentes aux traitements de données en général.

13. L'article 44 du RGPD pose comme principe l'interdiction des transferts de données vers des pays n'offrant pas un niveau de protection adéquat.

Différents régimes permettent d'aboutir à ce niveau de protection adéquat, à différentes conditions. Des États non européens peuvent avoir mis en place un niveau de protection suffisant, leur permettant d'être reconnus (1.A) comme les entreprises établies aux USA peuvent également avoir adhéré à un ensemble de principes de protection des données négociés avec le Département du Commerce américain sous le nom de *Privacy Shield (1.B)*.

Les transferts vers un État tiers ou une organisation internationale[25] peuvent se faire si la Commission européenne a constaté, par voie de décisions qu'un État tiers, un territoire ou un secteur spécifique de cet État tiers ou l'organisation internationale concernée présente un niveau de protection adéquat (1). En l'absence de décision, le transfert ne peut se faire que moyennant des garanties appropriées offertes par le responsable du traitement ou par le sous-traitant, garanties coulées dans un instrument juridique contraignant, par exemple des clauses contractuelles (2A), des règles d'entreprise contraignantes (2B) ou des codes de conduite ou mécanisme de certification (2C). Le règlement prévoit enfin un certain nombre d'exceptions (2.D).

1. Vers des pays offrant un niveau de protection adéquat

A. RECONNAISSANCE DU NIVEAU DE PROTECTION

14. L'article 45 du règlement autorise la Commission européenne à décider qu'un État tiers (voire un territoire ou un secteur spécifique – comme le secteur privé ou un secteur économique particulier[26] – de cet État tiers) ou qu'une organisation internationale présente un niveau suffisant de protection des données, de telle sorte qu'aucune autorisation spécifique ne sera nécessaire pour transférer des données vers ces entités.

15. Le règlement formalise et étend les critères déjà examinés in concreto par la Commission ou les Autorités nationales pour déterminer si un état offre un niveau de protection adéquat (ou si des BCR sont valables au regard du droit européen). De manière générale à travers l'ensemble du RGPD, les procédures à suivre sont également détaillées afin de dégager des solutions cohérentes, par référence soit à la procédure de concertation contenue dans le règlement, soit à la procédure d'examen contenue dans le règlement 182/2011 sur le contrôle de la Commission par les États membres[27]. En l'occurrence, la procédure prévoit un avis préalable du Comité Européen de la Protection des Données (CEPD) et renvoie, pour les modalités pratiques de l'examen à la procédure décrite à l'article 5 du règlement 182/2011[28].

Dans son processus d'évaluation, la Commission devra particulièrement tenir compte des éléments listés à l'article 45, plus nombreux et plus précis que ceux contenus dans la directive 95/46.

La décision devrait préciser sa portée territoriale et, si possible, identifier l'Autorité indépendante de Protection des données.

Un document de travail wp254rev.01 du Groupe de travail de l'article 29, désormais CEPD, établit les critères de référence pour l'adéquation.

[25] Définie comme étant : *«une organisation et ses organes subordonnés régi par le droit international public ou tout autre organisme qui est mis en place par, ou sur la base d'un accord entre deux ou plusieurs pays».*
[26] Considérant 104.
[27] Règlement (UE) no 182/2011 du Parlement Européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission, *J.O.* L 55, 28 février 2011, p. 13-18.
[28] Article 93.2

16. Une intéressante nouveauté par rapport à la situation actuelle réside dans l'obligation pour la Commission de surveiller le déroulement effectif des transferts réalisés sur base de cette décision[29] et de vérifier que l'État tiers ou l'organisation internationale concernée présente **toujours** un niveau de protection adéquat. À défaut, la Commission peut entrer en discussion avec l'État tiers ou l'organisation en vue de trouver une solution et amender ou suspendre la décision, sans possibilité de rétroaction toutefois. La Commission peut également décider qu'un État tiers ne présente pas de niveau de protection adéquat et interdire les transferts vers ces États tiers, sous réserve de l'application des articles 46 à 49[30].

La modification ou la suspension de la décision doit également respecter la procédure décrite à l'article 5 du règlement 182/2011.

17. Outre les trois membres de l'Espace Économique Européen que sont la Norvège, le Liechtenstein et l'Islande, au jour de la rédaction des présentes, les pays suivants sont considérés par la Commission comme présentant un niveau de protection adéquat : la Suisse, le Canada (pour les traitements soumis à la loi canadienne «Personal Information Protection and Electronic Documentation Act» et pour les données relatives aux passagers aériens), Andorre, l'Argentine, les États-Unis (si le destinataire des données aux États-Unis a adhéré aux « principes du bouclier de sécurité», ou «Privacy Shield» ainsi que pour les données relatives aux passagers aériens), Guernesey, l'île de Man, les îles Féroé, Jersey, l'Australie (pour les données relatives aux passagers aériens), Israël, la Nouvelle-Zélande, l'Uruguay et le Japon.

Dans les limites éventuellement édictées par la Commission et dans les limites du champ d'application du RGPD, des données à caractère personnel peuvent donc être transmises vers ces pays à des fins de traitement, moyennant uniquement le respect de l'ensemble des règles encadrant la protection des données dans l'État membre de départ.

Dès lors, parmi les États dont sont ressortissants les membres de la CIB, si l'on excepte les pays de l'UE et de l'EEE, seuls le Canada (pour les traitements soumis à la loi canadienne «Personal Information Protection and Electronic Documentation Act» et pour les données relatives aux passagers aériens), les États-Unis (aux conditions ci-après) et la Suisse sont considérés comme offrant un niveau de protection adéquat.

Aucun pays africain n'est donc reconnu comme tel.

B. LE CAS PARTICULIER DES USA : LE NIVEAU DE PROTECTION ADÉQUAT PAR LE PRIVACY SHIELD

18. Les États-Unis d'Amérique adoptent une approche très différente en matière de protection de la vie privée[31] par rapport à celle adoptée par l'Union européenne. Les différences paraissent inconciliables, mais il ne saurait évidemment être question, pour l'un et l'autre, de se passer d'un tel partenaire économique.

Sur base des articles 25 § 5 et 6 de la directive 95/46, la Commission a négocié avec le Département du Commerce américain, dans le cadre de la mise en place, par celui-ci, d'un ensemble de principes de protection des données – dénommé Safe Harbor[32] – auxquels les entreprises américaines pouvaient adhérer.

19. L'adhésion aux principes du Safe Harbor par les entreprises relève de l'autorégulation. Les entreprises souhaitant adhérer aux principes déclarent qu'elles respectent ceux-ci et sont inscrites dans un registre tenu à jour par le Département du Commerce. Chaque année, les entreprises doivent procéder à une autocertification[33] ou faire appel à un organisme certificateur externe.

[29] Y compris pour les décisions prises antérieurement, sur base des articles 25.6 et 26.4 de la Directive Vie Privée, considérant 106.
[30] Considérant 106.
[31] V. à ce sujet le chapitre consacré aux USA dans F. GILBERT, «Global privacy and security law», New York Wolters Kluwer, 2014, Vol. 2, §65 et s.
[32] Traduit parfois par «sphère de sécurité».
[33] Un guide est disponible sur le site du Département du Commerce : http://www.export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_061613.pdf (visité le 9 septembre 2014).

Le Département du Commerce américain ainsi que les agences nationales européennes de protection des données étaient chargés de la vérification du respect effectif des principes du Safe Harbor en cas de plainte de personnes concernées par les traitements de données.

20. Dès leur mise en œuvre, les principes du Safe Harbor ont fait l'objet de nombreuses critiques de la part de la doctrine et de la société civile européenne, fustigeant notamment sa trop grande souplesse et son manque d'effectivité[34].

C'est ainsi qu'une procédure initiée par un étudiant en droit autrichien a entraîné la saisine de la Cour de justice de l'Union européenne, laquelle devait répondre à une question préjudicielle concernant la validité des principes du Safe Harbor.

Cet étudiant, utilisateur de Facebook, s'est inquiété auprès de l'Autorité de Protection des Données irlandaises de l'envoi, par Facebook Ireland (siège de Facebook en Europe), de ses données à caractère personnel aux USA, où elles pourraient être soumises à des mécanismes de surveillance de masse.

L'Autorité irlandaise l'a éconduit, indiquant être tenue, sur base de l'article 25.6 de la directive 95/46, de la décision de la Commission européenne du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique.

Saisie d'un recours, la Haute Cour de Justice irlandaise a alors posé une question préjudicielle à la Cour de Justice de l'Union[35]:

« Est-ce que, dans le cadre de l'examen d'une plainte qui a été fait à une Autorité de Contrôle des données, selon laquelle des données personnelles sont transférées vers un autre pays tiers (dans ce cas, les États-Unis d'Amérique), dont les lois et les pratiques qui ne contiendraient pas de protections adéquates pour la personne concernée, l'Autorité de Contrôle est liée par la décision de la Commission décidant du contraire ? Ou encore, est-ce que l'Autorité de contrôle doit mener sa propre enquête sur la question à la lumière des faits nouveaux survenus dans l'intervalle depuis que la décision de la Commission a été publié ?[36]*»* .

La réponse de la Cour de justice de l'Union européenne fut cinglante :
« 1) L'article 25, paragraphe 6, de la directive 95/46/CE du 29 septembre 2003, lu à la lumière des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46 relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, par laquelle la Commission européenne constate qu'un pays tiers assure un niveau de protection adéquat, ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, telle que modifiée, examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.
2) La décision 2000/520 est invalide.[37]*»*

[34] V. notamment, B. HAVELANGE, A.-C. LACOSTE, «Les flux transfrontaliers de données à caractère personnel en droit européen», *J.D.E.*, 10/2001, pp. 241 et s.; Y. POULLET, «Les Safe Harbor Principles - Une protection adéquate ?», Juriscom, 10 juillet 2000, http://www.droit-technologie.org/upload/dossier/doc/19-1.pdf.
[35] CJUE, Schrems, C-362/14, documents non encore publiés.
[36] Traduction libre. Version originale de la question : «*Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?*», High Court of Ireland, Case N° 2013/765JR, 16 juillet 2014, http://www.europe-v-facebook.org/Order_ADJ.pdf (visité le 14 septembre 2014).
[37] C.J.U.E, 6 octobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner, http://curia.europa.eu/juris/liste.jsf?language=fr&num=C-362/14

21. Une nouvelle décision sur l'adéquation du Dispositif du Bouclier de Protection des Données UE – États-Unis (« Bouclier de Protection des Données ») ou (« Privacy Shield »), a alors été adoptée par la Commission européenne le 12 juillet 2016 et est entrée en vigueur le 1er août 2016[38].

22. Les modifications entre cette décision et la première ont paru à certain, et en tout cas à Maximilien Schrems, un peu « cosmétique » dès lors qu'elle relève toujours de l'autorégulation avec fort peu de contrôle et eu égard au Cloud act par exemple qui entre en contradiction avec le RGPD et une seconde affaire, dite SCHREMS II, est de nouveau pendante devant la Cour[39].

2. Vers des pays n'offrant pas un niveau de protection adéquat

23. Des transferts de données vers des États non membres de l'Union européenne ou de l'EEE qui ne sont pas reconnus comme offrant un niveau de protection – la grande majorité des pays du monde – sont toutefois possibles moyennant quelques aménagements.

24. Un transfert pourra être autorisé pour autant que le responsable du traitement ou le sous-traitant offrent des garanties appropriées au moyen d'un instrument juridique contraignant.

Ces garanties peuvent être fournies au moyen des instruments visés à l'article 46 du règlement :

a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;
b) des règles d'entreprise contraignantes ;
c) des clauses types de protection des données adoptées par la Commission ;
d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission ;
e) un code de conduite approuvé conformément, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; ou
f) un mécanisme de certification approuvé, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par :
a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale ; ou
b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

Dans la plupart des hypothèses, aucune autorisation spécifique d'une Autorité de contrôle ne serait plus nécessaire une fois les garanties mises en place.

[38] https://www.privacyshield.gov
[39] http://curia.europa.eu/juris/liste.jsf?num=C-311/18

25. Les Autorités de contrôle seront tenues d'un devoir de coopération entre elles et avec la Commission. Le règlement prévoit à cet effet, en son article 50, un mécanisme de contrôle de la cohérence qui devra être activé avant la validation par la Commission de clauses contractuelles types émanant d'une Autorité de contrôle ou si les transferts négociés entre le responsable du traitement (ou le sous-traitant) et le destinataire des données sont liés aux activités de traitement de données qui portent sur des personnes concernées dans plusieurs États membres, ou sont susceptibles d'affecter sensiblement la libre circulation des données à caractère personnel dans l'Union.

Le règlement permet aux Autorités de contrôle de modifier, remplacer ou suspendre les autorisations données dans le cadre de cet article 46. De même pour la Commission, qui doit toutefois respecter la procédure de l'article 5 du règlement 182/2011.

A. CLAUSES CONTRACTUELLES

26. En vertu de l'article 26.4 de la directive 95/46, la Commission européenne pouvait arrêter des clauses contractuelles types qui, insérées dans un contrat conclu avec une entreprise située en dehors de l'Union européenne, permettent d'offrir les garanties suffisantes au regard des exigences de la directive 95/46.

La Commission s'est saisie de cette possibilité et a publié plusieurs décisions contenant ces clauses contractuelles:

- Transfert vers un responsable de traitement : Décision de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE (2001/497/CE), modifiée par la Décision de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers (2004/915/CE);

- Transfert vers un sous-traitant :
  - o Avant le 15 mai 2010 : Décision de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE (2002/16/CE);
  - o Après le 15 mai 2010 : Décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil (2010/87/UE).

27. Le mécanisme des clauses contractuelles types des articles 28.6 à 8 et 46 c et d est resté globalement identique au mécanisme actuel. La commission n'a toutefois pas encore pris de nouvelles décisions et ce sont toujours les mêmes clauses contractuelles types qui ont cours, la référence à l'ancienne directive devant être lue comme un renvoi au RGPD.

Une nouveauté réside dans la possibilité pour les Autorités nationales d'adopter de telles clauses contractuelles et de les faire adopter par la Commission, les rendant généralement applicables.

28. Aux termes de l'article 46.2 c) du RGPD, la reprise telle quelle des clauses contractuelles rédigées par la Commission européenne par les entreprises lie les États-Membres. Les entreprises peuvent toutefois proposer leurs propres clauses et une procédure peut être mise en place au niveau national pour examiner la conformité de celles-ci.

Les Autorités nationales européennes de protection des données sont chargées de vérifier le respect des clauses contractuelles types rédigées par la Commission[40].

[40] Article 46.3. À)

B. RÈGLES D'ENTREPRISE CONTRAIGNANTES (BCR)

29. Les règles d'entreprises contraignantes[41] sont des règles internes mises en place au sein d'entreprises multinationales. Elles visent la mise en place, à l'intérieur d'un groupe de sociétés, d'un cadre global, conformes à la législation européenne, des traitements de données à caractère personnel. Les transferts de données à l'intérieur de l'entreprise multinationale peuvent donc être réalisés, même si les pays dans lesquels les membres du groupe d'entreprise sont installés n'offrent pas un niveau de protection adéquat. Les BCR ne couvrent toutefois pas les flux de données en dehors de ce groupe.

Outre la possibilité de se conformer à la législation européenne en la matière en évitant de multiplier les contrats pour chaque transfert, les BCR sont également généralement utilisés comme un outil central de gestion de la vie privée au sein de l'entreprise.

30. Les règles d'entreprise contraignantes (BCR) sont une des garanties appropriées visées par l'article 46 du règlement, et l'article 47 y est intégralement consacré.

Elles sont définies à l'article 4.20 du règlement comme étant les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe.

31. Les BCR devront être approuvées par l'Autorité de contrôle «chef de file» (guichet unique ou «one stop shop»), selon le mécanisme de contrôle de la cohérence prévu à l'article 63 du règlement.

L'article 56 du RGPD et les lignes directrices du CEPD concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant (wp244rev.01) précisent les critères permettant de déterminer l'Autorité de contrôle «chef de file» auprès de laquelle la demande d'approbation des BCR devra être introduite. Il s'agit de l'Autorité de l'État membre dans lequel est situé l'établissement principal du responsable du traitement ou du sous-traitant demandeur.

Les critères d'approbation des BCR sont listés dans les paragraphes 1 et 2 de l'article 47.

Pour être approuvées, les BCR devront être juridiquement contraignantes et mises en œuvre concrètement par chaque membre du groupement d'entreprises. Elles devront conférer des droits effectifs aux personnes concernées par les traitements de données et comporter, au minimum :

a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés ;
b) elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel ; et
c) elles précisent au moins :

- la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités ;
- les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question ;

[41] Plus régulièrement désignées par leur traduction et leur acronyme en anglais, «*Binding Corporate Rules*» ou BCR.

- leur nature juridiquement contraignante, tant interne qu'externe ;
- l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;
- les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 79 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes ;
- l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause ;
- la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournis aux personnes concernées, en sus des informations visées aux articles 13 et 14 ;
- les missions de tout délégué à la protection des données, ou de tout autre personne ou entité chargée de la surveillance du respect des REC au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations ;
- les procédures de réclamation ;
- les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande ;
- les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle ;
- le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j) ;
- les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes ; et
- la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

Dans le futur, la Commission pourra expliciter ces différents points.

Le CEPD a adopté, à ce sujet, les documents suivants auxquels on se référera utilement :

- Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes (wp256rev.01)
- Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants (wp257rev.01)
- Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR (wp263rev.01)
- Recommendation on the approval of the Controller Binding Corporate Rules form (wp264)
- Recommendation on the approval of the Processor Binding Corporate Rules form (wp265)

C. CODES DE CONDUITE ET CERTIFICATION

32. Le règlement ajoute encore quelques possibilités de se ménager des garanties appropriées, comme la procédure de certification ou la mise en place de codes de conduites, sous réserve toutefois d'une autorisation préalable de l'Autorité Nationale de Contrôle pour chaque transfert.

33. Les codes de conduite comme le prévoit l'article 40 du règlement ont pour objectif de faciliter la vie des TPE et PME en leur proposant un équivalent «allégé» des BCR. Rédigés par les associations regroupant les responsables de traitement ou les sous-traitants, ces codes de conduite doivent permettre aux entreprises de mieux comprendre et de mieux intégrer leurs obligations au titre du règlement. Les projets de code de conduite seront soumis à l'Autorité de Contrôle compétente, laquelle émettra un avis sur l'adéquation du code avec la législation en la matière et le publiera en cas d'avis positif.

Un code de conduite pourra couvrir plusieurs États membres, mais devra alors être revu par le Comité Européen à la Protection des Données, qui enverra son avis en copie à la Commission, laquelle, le cas échéant, l'avalisera.

34. La certification visée à l'article 42 du règlement a également pour but d'aider les TPE et PME. L'article 42 encourage les Autorités nationales à mettre en place des mécanismes ou des labels de certification démontrant le respect, par les entreprises, de leurs obligations en la matière. Les certificateurs devront être agréés par l'Autorité de Contrôle et démontrer leur indépendance et leur expertise.

35. Ceux qui critiquent le Privacy Shield, critiqueront sans doute les codes de conduite et la certification (comme les BCR, d'ailleurs), dans la mesure où ils reposent également sur un mécanisme de l'autorégulation.

Toutefois, les États membres ont introduit des balises afin de s'assurer qu'ils contiennent des engagements juridiques et que ces outils doivent être approuvés (voy. par exemple, les articles 43.2 c) et d) du chapitre V).

Le CEPD a, par ailleurs, adopté les lignes directrices :

- 1/2018 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement 2016/679 ;
- 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR ;
- 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679

.

[42] Que ce soit dans une procédure judiciaire, dans une procédure administrative ou toute procédure à l'amiable, y compris les procédures devant les organismes de réglementation, considérant 111.

[43] Dans ce cas, le transfert ne doit pas porter sur la totalité des données personnelles ou des catégories de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes ayant un intérêt légitime, le transfert ne peut être effectué qu'à la demande de ces personnes ou si elles en sont les destinataires.

D. EXCEPTIONS

36. Les principes de restriction des transferts listés ci-dessus connaissent plusieurs exceptions dans des cas spécifiques, listées à l'article 49 du règlement.

Le CEPD a adopté des lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement 2016/679.

En l'absence de reconnaissance d'un niveau de protection adéquat, de garantie appropriée, un transfert de données sera toutefois possible pour autant que :

a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ;
b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;
d) le transfert est nécessaire pour des motifs importants d'intérêt public ;
e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice[42]; Cette disposition est évidemment essentielle au travail des confrères ;
f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce[43].

Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

V. Conclusions

37. La collecte des données à caractère personnel est soit subie (à l'utilisation des services) soit obligatoire (imposé par l'État pour des besoins d'identification de la personne ou des de sécurité nationale). Dans les deux cas, personne concernée se voit contraint par une machine puissante contre laquelle elle n'a d'autre choix que de subir.

Il revient donc aux États de garantir la protection des données de types divers, collectées à différents niveaux. Il est sidérant de voir les collecteurs de ces données les VENDRE à l'insu et/ou contre le gré des personnes concernées (usagers de services).

L'intervention des États devrait garantir un traitement transparent des données à caractère personnel exclusivement pour les finalités pour lesquelles elles sont collectées. Il est impérieux que les États, particulièrement africains, se dotent d'une loi pour encadrer les traitements de données à caractère personnel. Il faut également prévoir la création d'autorités de protection des données chargées d'assurer le contrôle et sanctionner les abus et tout manquement à la loi.

En plein essor de la quatrième révolution, celle du numérique, les États africains devraient prendre leur destin en main afin d'éviter de subir le même sort que lors des trois dernières révolutions notamment agricole et industrielle.

38. Nous plaidons donc pour l'adoption rapide par l'OHADA d'un acte uniforme relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

39. Les entreprises situées au Canada (pour les traitements soumis à la loi canadienne «Personal Information Protection and Electronic Documentation Act» et pour les données relatives aux passagers aériens), les États-Unis (à condition de respecter le cadre du Privacy Shield) et la Suisse peuvent sans difficulté majeure, traiter sur leur territoire des données soumises au RGPD.

40. L'acte uniforme relatif à la protection des données à caractère personnel que nous appelons de nos vœux pourra, à terme, être reconnu par la Commission européenne comme offrant un niveau de protection adéquat et permettre donc de mêmes transferts aisés.

41. Dans l'intervalle, mais également pour les responsables du traitement établis dans les autres États tiers, les responsables de traitement peuvent utiliser une des options offertes par le RGPD : par exemple des règles d'entreprise contraignantes, des clauses contractuelles types ou particulières, passer par le mécanisme de la certification ou l'adhésion à un code de conduite. Le règlement prévoit enfin un certain nombre d'exceptions que les entreprises, et leurs conseils membres de la CIB, pourront exploiter.

42. Une chose est sûre : le RGPD est exigeant, mais n'est qu'un cadre. Il autorise encore les traitements de données à caractère personnel dans l'Union européenne et dans le reste du monde.

Il convient néanmoins que les responsables du traitement situés dans les États tiers maîtrisent, avec leurs conseils, le RGPD. Ce sera bientôt la clef obligatoire pour continuer à traiter avec des entreprises européennes.

Nous espérons, par cette modeste contribution, avoir aidé nos confrères de la CIB à appréhender les règles du RGPD encadrant le transfert des données à caractères personnel.

Jean-François Henrotte
Avocat aux barreaux de Liège et de Bruxelles

Coco Kayudi
Bâtonnier du barreau de Kinshasa - Matete