

Le droit congolais face aux enjeux de protection de l'identité numérique : quel regard prospectif ?

**Blaise LOLEKA RAMAZANI,**

Membre du conseil d'administration de Droit-Numérique.cd
Avocat au Barreau de Kinshasa/Matete
Assistant à la Faculté de Droit de l'Université Pédagogique Nationale (UPN)
Apprenant en DEA à l'Université Catholique du Congo

MOTS-CLÉS

Identité numérique
Identification électronique
Donnée personnelle
Trace numérique
Oubli numérique
Mort numérique
Autodétermination informationnelle

Keywords :

Digital identity
Electronic identification
Personal data
Digital footprint
Digital oblivion
Digital death
Informational selfd
Determination

RÉSUMÉ

À l'ère du développement du *Web 2.0 et 3.0*, l'identité d'un individu n'est plus constituée que des données de l'état civil. Elle regroupe de nombreuses autres informations identifiantes exprimées sous la forme de données personnelles. Notre activité en ligne génère d'énormes quantités de données personnelles qui sont convoitées, tantôt par les géants du numérique pour des fins commerciales tantôt par des cybercriminels en vue de mener des actions illégales. C'est tout l'enjeu de « l'identité numérique ». Cet enjeu est lié aux nouvelles réglementations qui nécessitent de repenser les questions de protection de vie privée en droit. Ces réglementations visent à renforcer cette protection en donnant plus de contrôle aux individus sur leurs données personnelles. Elles ont introduit en droit congolais des nouveaux droits issus du droit comparé, comme les droits à l'oubli et à la mort numériques ainsi que le droit à l'autodétermination informationnelle.

ABSTRACT :

In the age of Web 2.0 and 3.0, an individual's identity no longer consists solely of civil status data. It encompasses a wide range of other identifying information, expressed in the form of personal data. Our online activities generate enormous quantities of personal data, which is coveted both by digital giants for commercial purposes and by cybercriminals for illegal activities. This is what "digital identity" is all about. This issue is linked to new regulations that require us to rethink privacy protection issues in law. These regulations aim to reinforce this protection by giving individuals greater control over their personal data. They have introduced into Congolese law new rights derived from comparative law, such as the right to digital oblivion and death, and the right to informational self-determination.

INTRODUCTION

1 - La reconnaissance de la personnalité juridique à une personne physique assure son insertion dans la société globale et sa [re]connaissance par celle-ci.¹ Il est évident de pouvoir individualiser tout être humain, par rapport à tous les autres, ses semblables. Identifier une personne signifie la distinguer d'une autre², l'individualiser dans la société.³ Dans l'identification se loge l'idée de l'identité. L'identité⁴ se comprend comme un ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation...)⁵ Les éléments de l'identité d'une personne sont les attributs traditionnels émis par les autorités publiques (état civil, carte d'identité, passeport, permis de conduire, numéro de sécurité sociale, etc.). Il s'agit là des éléments stables de la personne au

¹ F. TERRE, *Introduction générale au droit*, 4^e éd., Dalloz, Paris, 1998, p. 328.

² G. CORNU, *Vocabulaire juridique*, 12^e éd., PUF Quadrige, Paris, 2018, p. 1109.

³ F. AMELI, *Droit : introduction, les personnes, les biens*, Montchretien, Paris, 2000, p. 146, cité par AMISI HERADY, *Droit civil : les personnes, les incapacités, la famille*, Vol.1, 4^e éd., EDUPC, Kinshasa, 2016, p.68.

⁴ Le mot « identité » tire sa source du mot latin « *idem* » qui veut dire « le même ».

⁵ S. GUINCHARD et T. DEBARD, *Lexique des termes juridiques*, 25^e éd., Dalloz, Paris, 2017-2018, p. 1082.

sens purement classique.

2 - À l'ère actuelle du tout numérique, le développement exponentiel du commerce électronique, des banques en ligne, des démarches administratives dématérialisées, des environnements numériques de travail, rendent nécessaire une « réidentification » ponctuelle de l'individu.⁶ Les méthodes d'identification d'une personne ont considérablement évolué au fil des siècles, dépassant largement le cadre traditionnel de l'état civil. On associe désormais, de nombreuses autres informations identifiantes des activités de notre vie, toutes exprimées sous la forme de données à caractère personnel.⁷ Ces informations sont de plusieurs ordres et peuvent être associées à l'état civil (adresse, date de naissance, etc.), à la sécurité (mot de passe ou code PIN), aux prestations contractuelles (numéro de contrat, de client), aux engagements financiers (n° de compte ou de la carte de crédit), à la vie numérique (n° de téléphone, adresse IP, etc.), aux marquages biométriques (photos, empreintes, etc.), ou encore à la connaissance partagée (votre musique préférée) de notre identité physique. Il s'agit là de l'« identité numérique ».

3 - L'identité numérique regroupe l'ensemble de données constituées par des éléments d'information et de preuve numérique et qui permettent d'identifier une personne sur les réseaux numériques mais, aussi potentiellement ailleurs.⁸ Elle est constituée de l'ensemble des traces numériques qu'une personne laisse sur Internet. À ce titre, trois types de traces numériques permettent de régénérer notre identité numérique en ligne. Le premier type concerne les informations partagées par l'individu lui-même (identité déclarative). Ces informations ont pour caractéristiques d'être conscientes, volontaires et plus ou moins contrôlées par leur producteur. Le deuxième type concerne les traces de navigation, plus ou moins conscientes et involontaires (identité calculée). Le simple fait de naviguer sur Internet produit ces traces de connexion (cookies) sur les différents sites Internet visités. Le troisième type n'est plus produit par l'individu mais, par d'autres internautes (identité agissante). Ce sont des informations diffusées par des tiers à notre propos. Ces informations sont le fruit de l'interaction entre un individu et ses interlocuteurs.

L'arrivée des identités numériques vient symboliser une nouvelle relation sociale, économique

⁶ E. NETTER, *Numérique et grandes notions du droit privé : la personne, la propriété, le contrat*, Mémoire en vue de l'habilitation à diriger des recherches en droit privé, présenté et soutenu publiquement le 20 novembre 2017, Garante : Judith ROCHFELD, Université de Picardie - Jules Verne, 2017, p. 56.

⁷ GUY DE FELCOURT, *L'usurpation d'identité ou l'art de la fraude sur les données personnelles*, CNRS Edition, Paris, 2011, p. 115.

⁸ *Idem*, p. 279

et politique qu'en tant qu'individu, nous entretenons avec notre environnement. Ces identités ont pour objectif de développer et de renforcer la confiance au sein de la sphère numérique globale, afin que les actes d'administration, de commerce, de vie civique ou d'échange entre deux personnes puissent y avoir le même degré de formalisme, de valeur probante et de sécurité.⁹ Dans cette logique, bon nombre des États se sont lancés dans la mise en place des systèmes nationaux d'identité digitale (SNID). Le SNID permet de fournir une identité légale à tous les résidents et/ou citoyens grâce aux outils numériques. Il est une plateforme intersectorielle qui permet d'établir, en peu de temps, un solide système d'identification, et d'offrir des services par voie électronique dans tous les secteurs de la vie.¹⁰ Néanmoins, les informations identitaires qui se [re]trouvent à la portée de tous sur Internet, constituent un danger permanent pour les utilisateurs et pour la protection de leur vie privée garantie aux articles 31 de la Constitution congolaise du 18 février 2006¹¹, 126¹² et 131¹³ de la loi n°20/017 du 25 novembre 2020 relative aux télécoms et aux TIC ainsi que les dispositions pertinentes de l'ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique. Ce danger est lié non seulement au vol de données identitaires, à l'usurpation d'identité mais aussi et surtout, à l'atteinte à la réputation des personnes et à leur vie privée.

4 - Les mécanismes de protection des données identitaires concernent tant les pouvoirs publics, les organismes privés que les individus eux-mêmes. Pour les pouvoirs publics, les barrières d'ordre public sont déployées sans qu'une initiative particulière soit nécessaire de la part de l'individu protégé. Ainsi, plusieurs instruments juridiques et techniques permettent aux individus de bien gérer et de protéger leur « avatar numérique¹⁴ ». Les enjeux associés à l'identité numérique sont liés aux nouvelles réglementations qui nécessitent de repenser les questions de vie privée en droit congolais. Par ailleurs, d'autres droits inspirés du droit comparé ont émergé en droit congolais, parmi lesquels figurent les droits à l'oubli et à la mort numériques ainsi que le droit à l'autodétermination informationnelle.

5 - Cependant, il est essentiel de comprendre le concept « identité numérique » et la façon

⁹ GUY DE FELCOURT, *op.cit.*, p.281.

¹⁰ Banque Mondiale, « Guide de l'identité électronique : À l'intention des parties prenantes d'Afrique », juin 2014, p. 4.

¹¹ Article 31, Constitution du 18 février 2006 telle que modifiée par la loi no 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006, in JO RDC, 52^e année, n° spécial, du 05 février 2011 : « Toute personne a droit au respect de sa vie privée et au secret de la correspondance, de la télécommunication ou de toute autre forme de communication. Il ne peut être porté atteinte à ce droit que dans les cas prévus par la loi ».

¹² Article 126, al. 1, loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication in JO RDC, 62^e année, n° spécial, du 22 septembre 2021 : « Toute personne a droit au secret des correspondances émises par voie de télécommunication et des technologies de l'information et de la communication [...] ».

¹³ Article 131, loi n° 20/017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc. : « La confidentialité des données à caractère personnel est garantie et protégée par la présente loi [...] ».

¹⁴ Un « avatar numérique » désigne la représentation informatique d'un internaute.

dont ses composantes fonctionnent dans différents médias (I), afin de déterminer les mécanismes de protection appropriés (II).

I. LES ESSENTIELS DE L'IDENTITE NUMERIQUE ■

6 - La compréhension du concept « identité numérique » commande que soient d'abord précisées les notions de base y relatives (A). C'est ensuite qu'il faut examiner les atteintes portées à cette nouvelle forme d'identité, ainsi que leurs modes de répression (B).

A. De l'identité à l'identité numérique

7 - Le concept « identité », vient du grec *idem*, dérivé du verbe être et signifie « le même ».¹⁵ L'égalité Je=Moi qui en découle conduit à faire de l'identité un agrégat composé d'une recombinaison d'ADN, d'une filiation familiale et sociale et d'un héritage matériel et symbolique.¹⁶ Classiquement, l'identité est l'ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique dans la société, au regard de l'état civil : nom, prénom, date de naissance, filiation, etc.¹⁷ L'étude de la notion de l'identité numérique ne peut se faire sans comprendre les liens de l'identité avec l'état civil. Ce dernier s'entend comme l'ensemble des qualités juridiques qui établissent la situation d'une personne au sein de la famille et de la société au point de vue de la jouissance et de l'exercice des droits civils.¹⁸ L'état civil permet de gérer avec une certaine efficacité l'identification et la reconnaissance des droits et devoirs attribués aux individus. Aussi, on pouvait considérer que vérifier l'identité d'une personne consisterait surtout à reconnaître ses éléments d'état civil, au travers d'un acte dressé par l'Officier de l'état civil.

8 - Cependant, la généralisation de l'usage d'Internet et le développement simultané du *web 2.0* avec l'apparition des réseaux sociaux numériques ont conduit à l'apparition d'une présence numérique pour les internautes : « l'identité numérique ». Constituée d'une superposition d'identités faites de données personnelles, déclaratives et comportementales, cette nouvelle forme d'identité est caractérisée par des modes d'expression de soi divers particulièrement visibles sur les réseaux sociaux numériques.¹⁹ D'où, définir l'identité numérique paraît primordiale, avant d'élucider les composantes de celle-ci.

1. La définition de l'identité numérique

9 - À l'image de l'identité, l'identité numérique regroupe dans une acception courante nos adresses IP ou e-mails, pseudonymes, URL, avatars informatiques ou toutes autres données permettant de nous identifier en ligne.²⁰ Elle est l'ensemble des contenus publiés sur Internet qui permettent de définir un individu. Elle regroupe aujourd'hui des contenus mis en ligne sur diverses plateformes [numériques], notamment sur les médias sociaux : blogs personnels,

¹⁵ G. CORNU, *Vocabulaire juridique*, 12^e éd, PUF Quadrige, Paris, 2018, p. 1109.

¹⁶ J.C. KAUFMANN, *L'invention de soi, une théorie de l'identité*, Hachette littératures, Paris, 2004. Cité par A. DUFOUR BAIDOURI, *L'identité numérique : un levier d'innovation pour les marques ?*, Thèse de doctorat en Science de l'Information et de la Communication présentée et soutenue publiquement le 4 décembre 2013, Université Panthéon Assas, sous la dir. Prof. Francis Balle, Paris, 2013, p. 35.

¹⁷ G. CORNU, *op.cit.*, p. 1109.

¹⁸ N. BOMPAKA, *Cours de droit civil : les personnes*, Faculté de Droit, UNIKIN, Kinshasa, p. 11. [inédit]

¹⁹ A. DUFOUR BAIDOURI, *op.cit.*, p. 3.

²⁰ GUY DE FELCOURT, *op.cit.*, p. 106.

profils sur les réseaux sociaux, contenus partagés, commentaires, etc. On distingue à cet effet deux types de contenus : ceux maîtrisés par la personne concernée (publiés par elle-même) et ceux non-maîtrisés par la personne concernée, c'est-à-dire publiés par un tiers.²¹

10 - L'identité numérique est formée de trois composantes complémentaires : l'identité déclarative, l'identité agissante, et l'identité calculée. L'« identité déclarative » se compose des informations de base de l'individu comme le nom, l'âge ou le sexe par exemple. Ces informations sont saisies directement par l'utilisateur lui-même, notamment au cours de la procédure d'inscription au service comme lors de la création d'un compte Facebook par exemple. L'« identité agissante » est constituée des messages répertoriés par le système, concernant les activités de l'utilisateur. C'est le fruit de l'interaction entre l'internaute et ses interlocuteurs comme les indications de l'activité telle que *x* et *y* sont désormais amis. « L'identité calculée » se compose des traces de navigation constituées de chiffres, produits du calcul du système, qui sont dispersés sur le profil de l'utilisateur²² comme le nombre d'amis ou le nombre de groupes auxquels il appartient. Dans le *Web 2.0*, ces trois composantes sont concomitantes et articulées entre elles.²³

11 - Les composantes essentielles de l'identité sont relativement faciles à saisir. Elles reposent généralement sur des attributs fixes et vérifiables, officiellement communiqués et enregistrés auprès des autorités publiques. Ces attributs comprennent les noms de l'individu concerné, la date et le lieu de naissance, les noms de ses parents et, dans certains pays, le numéro de sécurité sociale attribué à l'individu. On peut également identifier les individus au moyen de divers autres attributs tels qu'un nom d'utilisateur et un mot de passe informatique, une page Internet, un blog, une adresse IP (Internet Protocol) qui identifie chaque appareil connecté, une adresse de courrier électronique, un compte bancaire ou un numéro d'identification personnel (PIN).

12 - Par ailleurs, le législateur congolais a préféré le terme « identification digitale » par rapport à l'« identité numérique ». L'article 2 point 42 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique définit l'identification électronique comme un processus qui consiste à l'utilisation des données et éléments constitutifs de l'identité d'une personne physique ou morale, par des procédés électroniques qui représentent de manière univoque la personne physique ou morale concernée.

13 - L'identité apparaît alors transversale au sein de ces composantes. Toutefois, elle ne doit pas leur être assimilée au risque de confondre identité et identifiants, voire identité et profils ou « apparences » numériques.²⁴ D'une manière ou d'une autre, toutes ces composantes s'expriment sous forme de données personnelles qu'il convient d'analyser.

²¹ TH. COËFFE, « Qu'est-ce que l'identité numérique ? », in Regionsjob, 08 décembre 2014 - Mis à jour le 17 novembre 2015, disponible sur : [https://www.regionsjob.com/conseils/identite-numerique-definition.html] (consulté le 11 janvier 2022).

²² F. GEORGES, « L'identité numérique sous emprise culturelle : De l'expression de soi à sa standardisation » in Les Cahiers du numérique 2011/1, Vol. 7, pp. 3-48. Disponible sur : [https://www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-31.htm] (consulté le 11 janvier 2022).

²³ F. GEORGES, « L'Approche statistique de trois composantes de l'identité numérique dans Facebook », in F. MILLERAND, S. PROULX, J. RUEFF (sous la dir.), *Web social : Mutation de la communication*, PUQ, Québec, 2010, pp. 190-228.

²⁴ J. EYNARD (sous la dir.), *L'identité numérique : quelle définition pour quelle protection ?*, Larcier, Paris, 2020, p. 23.

2. Les données personnelles : nouvelle forme d'identité

14 - Dans notre environnement d'aujourd'hui, les informations relatives à l'identité ne sont pas seulement liées aux données de l'état civil. On y ajoute également plusieurs autres informations des activités de notre vie courante. Ces informations sont toutes exprimées sous la forme de données à caractère personnel. Comme nous l'avons indiqué supra, ces informations identitaires peuvent prendre plusieurs formes et sont associées notamment à l'état civil, à la sécurité, aux prestations contractuelles, aux marquages biométriques, ou encore à la connaissance partagée de notre identité physique.²⁵

15 - Sur le plan juridique, le rapport entre identité et données personnelles est déjà reconnu puisque la législation établit formellement le lien entre information « identifiante » et données personnelles. Dans les faits, ce lien remonte en France avec la loi informatique et libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004. Cette loi définit la donnée personnelle comme « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».²⁶

16 - Dans la même approche, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) définit la donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».²⁷ La particularité du RGPD est qu'il ajoute les définitions des données biométriques et des données de santé tout en complétant la notion des données génétiques.²⁸

17 - S'inspirant des législations européenne, africaine²⁹ et française, le législateur congolais définit les données à caractère personnel comme « toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propre à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique³⁰ ». Sans contredire la loi n°20/017 du 25 novembre 2020 relative aux télécommunications, l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique abonde dans le même sens en définissant les données personnelles comme toute information se rapportant à une personne physique identifiée ou identifiable

²⁵ GUY DE FELCOURT, *op.cit.*, p. 115.

²⁶ Article 2, loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004.

²⁷ Article 4-1, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

²⁸ Article 4.13-15, Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, préc.

²⁹ Au niveau africain, la convention de l'Union Africaine du 27 juin 2014 sur la cybersécurité et la protection des données à caractère personnel définissait déjà les données à caractère personnel dès 2014 comme « toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité ».

³⁰ Article 4.37, loi n°20/017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

directement ou indirectement.³¹ Ces deux définitions ont le mérite d’englober les informations permettant d’identifier la personne directement (nom, sexe, adresse, etc.) et indirectement (n° de téléphone, n° d’identification, données de localisation, etc.). Elles établissent un lien suffisant entre identité et données personnelles.

18 - Pour J. Eynard, la donnée personnelle devrait être comprise comme toute information saisissant l’essence physique ou psychique de la personne physique identifiée ou identifiable qu’elle concerne et échappe intellectuellement et juridiquement à cette dernière.³² Puisque la donnée concerne l’individu, il est primordial de s’interroger sur le lien unissant la donnée à son porteur et de la capacité de ce dernier à la protéger en pratique. Plusieurs avis se dégagent. Certains auteurs ont qualifié ce lien de droit de la personnalité³³, d’autres de droit de la propriété.³⁴ La première qualification a dû être écartée en raison du caractère disponible de la donnée personnelle. Retenir cette qualification aurait en effet conduit à admettre un affaiblissement de la protection assurée par les droits de la personnalité.³⁵ Quant à la qualification de droit de propriété, elle n’a pas non plus convenu. Du fait de la titularité de l’*abusus* par le propriétaire, elle aboutirait à admettre une disposition totale de la personne sur ses données personnelles.

19 - Le rejet du droit de la personnalité et du droit de propriété a débouché à l’adoption du droit à l’ « autodétermination informationnelle ». Ce droit est l’œuvre de la jurisprudence allemande depuis les années 1983 ainsi que de la Charte des droits fondamentaux en Europe³⁶. Selon ce principe, chacun devrait avoir le contrôle de tous les traitements relatifs à ses données, garder le pouvoir sur les usages qui en sont faits, les administrer, ceci pendant toute la durée des traitements.³⁷Nous y reviendrons.

20 - La constitution de notre identité a donc profondément changé. Désormais, elle s’exprime dans bien de cas, sous la forme de données personnelles. Non seulement ces données s’affranchissent de leur support documentaire, mais elles vont plus loin dans la diversité des champs d’expression et d’application, grâce à leur immatérialité.³⁸ De ce fait, sans que nous en ayons toujours conscience, elles viennent radicalement modifier notre rapport à autrui. L’identité numérique et l’état civil sont donc intimement liés, car nos données personnelles sont devenues l’expression pratique de notre identité dans la quasi-totalité des circonstances de la vie en société. Toutefois, une fois établi le cadre de la nouvelle identité par les données, il s’observe l’inquiétante recrudescence de la fraude identitaire en ligne.

B. Les atteintes à l’identité numérique

21 - Les atteintes à l’identité sont considérées aujourd’hui comme un des risques majeurs auxquels s’exposent les consommateurs et les utilisateurs dans l’environnement numérique. Les

³¹ Article 2.30, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, JO RDC, numéro spécial, 64e année, 11 avril 2023.

³² J. EYNARD, *Les données personnelles : quelle définition pour un régime de protection ?*, Michalon, Coll. Essai, Paris, 2013, p. 189.

³³ P. CATALA, « Ébauche d’une théorie juridique de l’information », Dalloz, 1994. N. MALLEY-POUJOL, *Droit à et sur l’information de santé*, cité par J. EYNARD, *Les données personnelles : quelle définition pour un régime de protection ?*, *op.cit.*, p. 189-190.

³⁴ F. ZENATI-CASTAING et T. REVET, *Manuel de droit des personnes*, PUF, Coll. Droit Fondamental, Paris, 2006.

³⁵ J. EYNARD, *Les données personnelles : quelle définition pour un régime de protection ?*, *op.cit.*, p. 189.

³⁶ Article 8, Charte des droits fondamentaux de l’UE du 7 décembre 2000. Son équivalent en droit congolais est l’article 31 de la Constitution du 18 février 2006.

³⁷ K. NDUKUMA ADJAYI (sous la dir.), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du commerce électronique : enjeux civils, consommateurs, cyber-criminels, d’extranéité et de déterritorialité*, L’Harmattan, coll. « Enjeux et droits numériques », Paris, 2021, p. 84.

³⁸ GUY DE FELCOURT, *op.cit.*, p. 116.

situations de vol de données identitaires, d'usurpation d'identité et de tromperie sont fréquemment rencontrées et qu'il importe, dès lors, d'en définir leur portée.

1. *Le vol de données [identitaires]*

22 - Selon l'OCDE³⁹, le vol d'identité correspond à « l'acquisition, le transfert, la possession ou l'utilisation non autorisés des informations personnelles d'une personne physique ou morale dans l'intention de commettre, ou en relation avec, des actes frauduleux ou autres délits⁴⁰ ». Bien que cette définition englobe à la fois les individus et les personnes morales, la portée de la présente étude se limite au vol d'identité affectant les consommateurs (personnes physiques). Cette définition s'applique, quel que soit le support au moyen duquel le vol d'identité est perpétré.⁴¹ De manière générale, les voleurs d'identité emploient diverses méthodes pour obtenir les informations personnelles de leurs victimes. Parmi ces méthodes figurent : le *spamming* qui consiste à l'envoi de courriers électroniques indésirables ; le *phishing* ou l'hameçonnage qui consiste à envoyer un e-mail non sollicité à une personne dans le but d'obtenir ses coordonnées confidentielles⁴² ; le *pharming* qui consiste à rediriger les utilisateurs d'un site web authentique vers un site web frauduleux à partir duquel, les données personnelles sont volées.⁴³

23 - En droit congolais, le vol des données [identitaires] est sanctionné par la loi du 25 novembre 2020 sur les télécoms et les TIC. Son article 196 assimile au vol prévu par le code pénal ordinaire, toute soustraction frauduleuse d'information à travers un système de communication électronique au préjudice d'autrui. L'infraction de vol elle-même est prévue à l'article 79 du code pénal en ces termes : « *Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol* ». L'article 80 du même code prévoit la peine de cinq ans de servitude pénale et/ou d'une amende de vingt-cinq à mille zaires pour le vol simple.

24 - En France par ailleurs, l'article 434-23 du code pénal punit « *le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales* ». Cette incrimination vise « *le nom d'un tiers* » correspondant à l'identité d'une personne réellement existante. Selon É. Caprioli, « *le nom d'un tiers* » doit s'entendre comme l'un des attributs de la personne au sens du Code civil.⁴⁴ Ainsi, cette disposition protège aussi bien les éléments de l'identité civile que de l'identité numérique de l'individu. Au final, seule compte le vol du nom d'un tiers peu importe le support utilisé, y compris sur Internet.

25 - Aujourd'hui, l'économie de la cybercriminalité vaut des milliards de dollars et compte beaucoup de participants et d'éléments constitutifs. Parfois, les voleurs d'identité n'utilisent pas eux-mêmes l'identité de la victime pour commettre une fraude. Ils la vendent dans le *dark*

³⁹ Organisation de coopération et de développement économique.

⁴⁰ OCDE, « Document exploratoire sur le vol d'identité en ligne », juin 2008, p.5. Disponible sur : [https://www.oecd.org.stiPDF], (consulté le 17 janvier 2022).

⁴¹ *Idem*, p. 6.

⁴² K. NDUKUMA ADJAYI (sous la dir.), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du commerce électronique : enjeux civils, consommateurs, cyber-criminels, d'extranéité et de déterritorialité*, op.cit, p. 313.

⁴³ *Idem*, p. 314.

⁴⁴ É. CAPRIOLI, « De l'usurpation d'identité en matière pénale », sous Crim. 29 mars 2006, n° 05-85.857 : Bull. crim. n° 94 ; CCE n° 7, juill. 2006, comm. 117. Cité par É. STELLA, *L'adaptation du droit pénal aux réseaux sociaux en ligne*, Thèse en vue de l'obtention du grade de Docteur en droit privé et sciences criminelles présentée et soutenue publiquement le 12 décembre 2019, sous la dir. Frédéric STASIAK, Université de Lorraine, Lorraine, 2019, p. 163.

*web*⁴⁵, à d'autres personnes. Ces dernières pourront soit commettre elles-mêmes la fraude, soit générer de nouvelles formes illégales d'identité personnelle (comme un certificat de naissance, un permis de conduire ou un passeport). Le vol d'identité peut, dans certaines circonstances, être pris comme un élément constitutif d'autres atteintes ou délits. C'est notamment le cas où le voleur d'identité utilise à sa guise, l'identité volée, faisant ainsi apparaître l'infraction d'usurpation d'identité.

2. L'usurpation d'identité [numérique]

26 - L'une des conséquences du changement de mode d'expression de notre identité consiste en ce que, ce sont dorénavant les données personnelles qui nous représentent et nous habillent, l'imposture s'est fait transformée en une simple fraude sur les données. Selon l'auteur Guy De Felcourt, usurper l'identité consiste simplement à utiliser frauduleusement les éléments d'information susceptibles de déterminer à la fois l'unicité (un parmi plusieurs) et parfois l'authenticité (celui qu'il prétend être) d'une personne.⁴⁶ En d'autres termes, l'usurpation d'identité se [re]trouve dans le comportement de quelqu'un qui s'attribue une identité à laquelle il ne peut prétendre.⁴⁷ L'usurpation d'identité devient pénalement répréhensible lorsque ce comportement devient préjudiciable soit à l'égard de la personne dont l'identité a été usurpée, soit pour les tiers trompés par l'emploi de la fausse identité.

27 - L'usurpation d'identité se présente comme un délit qui désigne l'utilisation d'informations personnelles permettant d'identifier une personne sans son accord pour réaliser des actions frauduleuses. En pratique, ces informations peuvent être obtenues par les cybercriminels de plusieurs manières notamment à suite à la perte ou au vol de documents d'identité de la victime, par le biais d'un message d'hameçonnage (*phishing*), par le piratage d'un de ses comptes en ligne ou d'un de ses appareils ou encore le piratage d'un site Internet sur lequel ses informations sont hébergées.

28 - Les usurpateurs d'identité exploitent les informations personnelles de leurs victimes afin d'accomplir divers agissements illégaux. Généralement, ces agissements consistent à utiliser frauduleusement des comptes existants, à ouvrir de nouveaux comptes, à obtenir frauduleusement des allocations, services ou documents des administrations publiques, à frauder en matière de soins de santé ou à négocier des données personnelles sans autorisation⁴⁸ ou obtenir tout avantage quelconque au nom de la victime.

29 - En droit congolais, avant l'avènement de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, l'infraction d'usurpation d'identité [numérique] n'était pas explicitement prévue dans le code pénal. Cependant, son auteur pouvait être sanctionné sur base de l'article 69 du code de la famille. Cet article se limite uniquement à punir l'usurpation volontaire

⁴⁵ Le « *Dark Web* » ou le web clandestin est un ensemble caché de sites Internet accessibles uniquement par un navigateur spécialement conçu à cet effet. Il est utilisé pour préserver l'anonymat et la confidentialité des activités sur Internet. Si certains l'utilisent pour échapper à la censure gouvernementale, d'autres s'en servent également pour mener des activités hautement illégales.

⁴⁶ GUY DE FELCOURT, *op.cit.*, p. 117.

⁴⁷ C. LACROIX, « Rép. Pén », Dalloz, juin 2012, V° usurpation d'identité, n°1, cité par E. STELLA, *L'adaptation du droit pénal aux réseaux sociaux en ligne*, *op.cit.*, p. 158.

⁴⁸ OCDE, « Document exploratoire sur le vol d'identité en ligne », *op.cit.*, p. 6.

et continue d'un nom d'un tiers. La peine prévue est de sept jours à trois mois de servitude pénale et/ou d'une amende de 500.000 à 1.000.000 de francs congolais.

30 - À ce jour, l'usurpation d'identité est prévue et sanctionnée par l'article 351 de l'ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique. Cet article incrimine le fait d'usurper l'identité d'autrui ou les données permettant de s'attribuer faussement et de manière illicite l'identité d'autrui dans le but de troubler sa tranquillité, de porter atteinte à son honneur, à sa considération ou à ses intérêts. L'auteur est puni d'une servitude pénale allant d'un à cinq ans et d'une amende de 20 à 100 millions de francs congolais.⁴⁹ De même, celui qui aura transféré, possédé ou utilisé un moyen de s'identifier à une autre personne dans l'intention de commettre l'infraction, d'aider ou d'encourager une activité illégale est puni d'une peine de deux à cinq ans de servitude pénale et/ou d'une amende de 5 à 100 millions de francs congolais.⁵⁰

31 - À côté de l'infraction d'usurpation d'identité, le code du numérique sanctionne sous une autre forme l'utilisation frauduleuse des éléments d'identification dans le but de tromper les usagers d'un service de communication électronique. Ainsi, l'article 349 punit au titre de tromperie, le fait d'utiliser les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations confidentielles.⁵¹

32 - À titre comparatif, le code pénal français prévoit l'infraction d'usurpation d'identité [numérique]. Son article 226-4-1 punit d'un an d'emprisonnement et d'une amende de 15 000 €, « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ». Cette infraction est punie des mêmes peines lorsqu'elle est commise sur « *un réseau de communication au public en ligne* ». Introduite par la loi n°2011-267 du 14 mars 2011, dite « LOPPSI II », cette disposition démontre l'adaptation du droit français aux nouvelles formes d'atteintes à l'identité, y compris dans la sphère numérique. Elle offre une protection optimale de l'identité civile et numérique en ce sens qu'elle vise « *les données de toute nature permettant l'identification d'un individu* ». Le caractère globalisant de cette disposition permet d'inclure autant les éléments de l'identité civile d'une personne que ses attributs numériques.⁵²

II. LES ENJEUX DE PROTECTION DE L'IDENTITÉ NUMÉRIQUE ■

33 - Tenant compte de la complexité que revêt cette nouvelle forme d'identité, il se pose la question de savoir : à qui incombe la protection de l'identité numérique ? Pour y répondre, deux approches sont défendues. L'une consiste à dire que les individus sont incapables – par manque de compétence, de temps, et peut-être d'intérêt – de défendre eux-mêmes leur identité

⁴⁹ Article 351 al.1, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁵⁰ Article 351 al.2, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁵¹ Article 349, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁵² É. STELLA, *L'adaptation du droit pénal aux réseaux sociaux en ligne*, op.cit, p. 172.

numérique. Une telle analyse doit conduire à un droit des données à caractère personnel protecteur, dirigiste, et impératif. En revanche, la seconde approche voudrait qu'on laisse aux personnes concernées le soin de fixer elles-mêmes ce qui constitue un usage acceptable des informations qu'elles cèdent ou sèment derrière elles. Dans ce contexte, la réglementation serait alors libérale, simple et personnalisée.⁵³

34 - Le droit positif pour sa part, ne choisit pas entre ces deux approches. Il les combine. D'abord, bon nombre de règles s'imposent à ceux qui décident de manipuler les données entre autres : les responsables de traitement, leurs sous-traitants ainsi qu'à leurs partenaires. Ensuite, des moyens juridiques s'offrent aux individus eux-mêmes afin de contrôler, préserver et modeler leur identité numérique (A). Dans ce contexte, l'instauration d'un système national d'identification digitale en RD Congo dévient une nécessité (B).

A. La protection de l'identité numérique par les pouvoirs publics et par l'individu lui-même

35 - Si l'expression elle-même est récente en droit congolais, les prémisses de l'identité numérique en France sont clairement fixées aux années 1974 avec le projet SAFARI⁵⁴. Ce projet fut révélé le 21 mars 1974 par le journal Le monde, dans un article intitulé « safari » ou la chasse aux Français de P. Boucher.⁵⁵ Pour rappel, l'objectif de ce projet était d'identifier chaque Français et d'interconnecter tous les fichiers administratifs grâce à l'utilisation d'un identifiant unique, le numéro d'immatriculation au répertoire (NIR).

36 - À la suite d'une vive opposition populaire face à l'effet *Big brother*⁵⁶ qu'il contenait, ce projet fut abandonné et aboutit à la création de la Commission nationale de l'informatique et de libertés (CNIL) dont l'existence fut consacrée par la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La CNIL fut créée avec pour mission de réguler la donnée à l'aune des droits fondamentaux des individus. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.⁵⁷

37 - L'ambition de la loi Informatique et Libertés était de trouver un équilibre entre la libre circulation de l'information et la protection de la personne.⁵⁸ Son article 1^{er} dispose que : « l'informatique doit être au service du citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». Cet état de législation avait conféré aux pouvoirs publics la mission de protéger les données des citoyens, tout en reconnaissant aux individus un droit de contrôle effectif sur leurs données personnelles.

⁵³ E. NETTER, *Numérique et grandes notions du droit privé : la personne, la propriété, le contrat, op.cit.*, p. 84.

⁵⁴ SAFARI : Système automatisé pour les fichiers administratifs et le répertoire des individus.

⁵⁵ P. BOUCHER, « Safari ou la chasse aux Français », in *Le monde*, 21 mars 1974, p. 9.

⁵⁶ L'expression *Big brother* est directement tirée du célèbre ouvrage de George ORWELL, intitulé *1984*. Écrit en 1949. Ce roman d'anticipation décrit un État policier et totalitaire dans lequel la liberté d'expression est anéantie et une organisation très pointue permet la surveillance quotidienne du citoyen.

⁵⁷ [https://www.cnil.fr/fr/les-missions-de-la-cnil], (consulté le 16 février 2022)

⁵⁸ L. GRYNBAUM, C. LEGOFFIC et L. MORLET-HIDARA, *Précis de Droit des activités numériques*, 1^{ère} éd., Dalloz, Paris, 2014, p. 775.

1. La protection de l'identité numérique par les pouvoirs publics

38 - La protection de l'identité numérique est un enjeu majeur pour les pouvoirs publics à l'ère du tout numérique. Ceci est crucial pour la sécurité des citoyens à travers la protection de leurs données personnelles contre toute forme de menaces. L'intervention des pouvoirs publics établit une sorte de confiance dans l'utilisation des services en ligne tout en permettant à l'État de maîtriser les données nationales et préserver la sécurité des infrastructures numériques.

39 - Les techniques numériques mettent à l'épreuve la vie privée ainsi que les données personnelles. Le droit de la protection des données personnelles n'est pas laissé au seul droit de la personnalité ni assimilé au droit patrimonial.⁵⁹ Ce droit est généralement assuré par un « service public de la donnée », sans lequel le citoyen est désarmé vis-à-vis de la puissance économique et technologique des responsables de traitement.⁶⁰ Ceci passe par l'adoption de lois et de réglementations spécifiques de protection des données personnelles.

40 - Ainsi, le dispositif juridique congolais de protection des données personnelles est caractérisé par une dualité de régime, à savoir : le régime de la loi n° 20-017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication d'une part et celui de l'Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique d'autre part.

a. Bref aperçu du régime de la loi n° 20-017 du 25 novembre 2020 relative aux télécommunications et aux TIC

41 - La loi n° 20-017 du 25 novembre 2020 sous examen contient quelques innovations sommaires en termes de protection de la vie privée et des données à caractère personnel. Cette protection s'analyse dans la consécration pour chaque utilisateur du droit spécifique de bénéficiaire du secret de correspondances émises non seulement par la voie des télécommunications, mais aussi celles émises par la voie des TIC.⁶¹

42 - Hormis, la définition des données à caractère personnel prévue à l'article 4 point 37, l'article 131 de la loi n° 20-017 du 25 novembre 2020 du 25 novembre 2020 garantit la confidentialité des données à caractère personnel. Ainsi, tout traitement est subordonné au consentement préalable de la personne concernée ou à la réquisition de l'officier du ministère public. Et ce consentement, pour être valablement reçu, doit être libre, spécifique, éclairé, formulé en des termes clairs et simples et faciles d'accès.

43 - La loi impose également une protection spécifique à certaines catégories de données dites « sensibles » en interdisant leur collecte et traitement. Il s'agit des données qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou

⁵⁹ K. NDUKUMA ADJAYI, *Droits des télécoms et du numérique : Profil africain et congolais, prospective comparée d'Europe et de France*, tome II, l'Harmattan, Coll. Enjeux & Droits numériques, Paris, 2019, p. 239.

⁶⁰ *Ibid.*

⁶¹ Article 126, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.⁶²

44 - Par ailleurs, cette loi renvoie à un arrêté ministériel la fixation des conditions et modalités de collecte, d'enregistrement, de traitement, de stockage et de transmission des données à caractère personnel⁶³, tout en renforçant certaines dispositions pénales en cas de violation des règles en matière de protection de la vie privée et des données à caractère personnel.

45 - C'est ainsi que la loi punit de la même peine prévue en matière de violation de correspondance tout agent qui se rendrait coupable de violation du secret des correspondances ou de manipulation, sans autorisation préalable, des données à caractère personnel.⁶⁴ Dans la même optique, son article 190 punit de la même peine prévue en matière de violation de correspondance, toute personne qui procède ou fait procéder à un traitement des données à caractère personnel sans avoir obtenu l'autorisation préalable requise à l'article 126.⁶⁵

46 - En cette matière, l'article 72 du Code pénal congolais prévoit une servitude pénale d'un mois au plus et/ou d'une amende qui ne dépassera pas deux milles (zaïres). Au sens des articles 179 et 190 sus-évoqués, seul l'agent auteur de l'infraction encourt la peine de servitude pénale prévue à l'article 72 du code pénal en matière de violation de correspondance. Quand il s'agit d'un employeur, il sera condamné à une amende allant de 50.000.000 à 100.000.000 de francs congolais. Ces articles confèrent à la victime de l'infraction le droit de réclamer une réparation civile solidairement à l'agent auteur de l'infraction et à son employeur. Il en est de même de l'article 180 qui punit toute interception, écoute, enregistrement, transcription au moyen d'un quelconque dispositif pour divulgation d'une communication ou correspondance privée, d'une servitude pénale principale d'un à trois ans et/ou d'une amende de 1.000.000 à 10.000.000 de francs congolais.

47 - En sus, la loi n° 20-017 du 25 novembre 2020 avait confié la mission de régulation et de protection des données à caractère personnel à l'Autorité de Régulation des postes et télécommunications du Congo (ARPTIC).⁶⁶ Cette dernière fut créée en 2023 en remplacement de l'ancienne Autorité de régulation de postes et des télécommunications (ARPTC).⁶⁷

b. Bref aperçu du régime de protection des données personnelles du code du numérique

48 - La promulgation en mars 2023 de l'Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique avait marqué une étape significative dans la régulation du numérique en RD Congo. Elle a introduit un cadre juridique solide d'identification électronique des citoyens mais aussi, de protection des données personnelles. Ce cadre juridique vise à protéger et à sauvegarder le traitement des données personnelles (identitaires).

⁶² Article 132, al. 2, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc., équivalent de l'article 255 point 3, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁶³ Article 133, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

⁶⁴ Article 179, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

⁶⁵ Article 190, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

⁶⁶ Article 13 point 6, Loi n° 20-017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

⁶⁷ Cf. Décret n°23/13 portant création, organisation et fonctionnement de l'Autorité de régulation des Postes, des télécommunications et des TIC.

49 - Son régime de protection accorde aux individus des droits fondamentaux tels que le droit à l'information, le droit de communication, le droit d'opposition, le droit de rectification, le droit de suppression ou d'effacement, etc.⁶⁸ Il impose un certain nombre d'obligations strictes aux responsables de traitement telles que la transparence, la sécurité, la responsabilité, la conformité, etc.⁶⁹

50 - Le code du numérique établit, en outre, des principes fondamentaux de traitement des données personnelles notamment :

- *La déclaration préalable* : le traitement de données personnelles est soumis à une déclaration préalable auprès de l'autorité de protection des données⁷⁰ ;
- *La loyauté et la licéité des données* : les données sont loyales et licites si la personne concernée a donné son consentement préalable, si les données sont récoltées pour une finalité déterminée, explicite et légitime tout en respectant les principes de transparence⁷¹ et de respect de la dignité humaine, de la vie privée et des libertés publiques⁷² ;
- *La confidentialité des données* : les données personnelles sont traitées de manière confidentielle et protégée, y compris lorsque leur traitement nécessite leur transmission dans un réseau⁷³ ;
- *La limitation de la durée* : la durée de conservation des données personnelles ne doit pas dépasser celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou traitées, sauf exception⁷⁴ ;
- *La sécurité* : les données personnelles sont traitées de façon à garantir la sécurité appropriée.⁷⁵

51 - Le code du numérique a créé une Autorité de protection des données dénommée Autorité de protection des données (APD). Son organisation et son fonctionnement devraient être fixés par Décret du Premier Ministre.⁷⁶ L'APD a pour mission principale de veiller à ce que le traitement des données publiques et à caractère personnel soit conforme au Livre III de l'Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique.⁷⁷

52 - En attendant sa mise en place effective, les missions de l'APD ont été confiées provisoirement à l'ARPTIC/ARPTC par Arrêté ministériel du 17 août 2024 portant harmonisation des modalités de mise en œuvre des régimes de l'Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique et de la loi n° 20-017 du 25 novembre 2020 sur les télécoms et les TIC.⁷⁸

⁶⁸ Articles 209 à 218, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁶⁹ Articles 219 et suiv., Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁰ Articles 186 et suiv., Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷¹ Articles 192 et 193. 1, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷² Article 192 al. 2, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷³ Article 193.2, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁴ Article 193. 3, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁵ Article 193.4, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁶ Article 262, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁷ Articles 262 et 263, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁸ Lire à ce sujet BROZECK KANDOLO, « Régulation du numérique en RDC : l'ARPTIC investie Autorité unique pour la régulation du numérique, la certification électronique et la protection des données », Dossier n°4, in Droit-Numérique.cd, octobre 2024, disponible sur : [https://droitnumerique.cd/regulation-du-numerique-en-rdc-larptic-investie-autorite-unique-pour-la-regulation-du-numerique-la-certification-electronique-et-la-protection-des-donnees/], (consulté le 23 octobre 2024)

2. La protection de l'identité numérique par l'individu lui-même

53 - Comme dit précédemment, les articles 209 à 218 du code du numérique consacrent plusieurs droits au profit de l'individu dont les données sont traitées. Lorsque le traitement est mis en œuvre, le code du numérique crée, dans un souci de transparence, le droit d'être informé et d'accéder aux données.

54 - D'abord, la personne a le droit de savoir si le responsable d'un traitement utilise des données à caractère personnel la concernant. Le refus non justifié de donner cette information au requérant peut exposer le responsable du traitement à des sanctions. Ensuite, le droit d'être informé est complété par le droit d'accéder aux données traitées et d'obtenir, par conséquent, la communication d'un certain nombre d'informations permettant à la personne concernée de vérifier quelle est l'utilisation des données en cause. Le droit d'accès permet à tout individu de vérifier le caractère pertinent, adéquat et non excessif des données collectées et traitées au regard de la finalité poursuivie.

55 - De plus, la personne concernée doit pouvoir comprendre la finalité retenue par le traitement. Ceci implique l'obligation de communiquer les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé. Les informations demandées doivent être fournies de manière lisible. C'est ainsi qu'il est reconnu à l'individu concerné, le droit de rectification et même d'opposition afin de pouvoir maîtriser les données traitées.

56 - En plus des droits déjà mentionnés, nous assistons à l'émergence de nouveaux droits, comme le droit à l'autodétermination informationnelle et les droits à l'oubli et à la mort [numériques] qu'il convient d'analyser.

a. Le droit à l'autodétermination informationnelle

57 - Le droit à l'autodétermination informationnelle fut consacré par la Cour constitutionnelle fédérale allemande depuis 15 décembre 1983. Selon cette Cour, ce droit fondamental : « garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ». ⁷⁹ Cette position avait été reprise, en Europe, par la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 qui posait déjà le principe selon lequel toute personne a droit à la protection des données à caractère personnel la concernant. ⁸⁰ Le règlement européen du 27 avril 2016 y fait également allusion dans son considérant 7 en disposant que : « *les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant* ⁸¹ ». Selon ce principe, tout individu devrait avoir le contrôle de tous les traitements relatifs à ses données, garder le pouvoir sur les usages qui en sont faits, les administrer, ceci pendant toute la durée des traitements. ⁸²

⁷⁹ Cour constitutionnelle fédérale Allemande, 15 déc. 1983, relativement à une loi sur le recensement : le principe fut déduit des articles 1^{er} (dignité de l'homme) et 2^e (droit au libre développement de sa personnalité) de la Loi fondamentale et implique que « la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ».

⁸⁰ Article 8, Charte des droits fondamentaux de l'UE : 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

⁸¹ Considérant 7 du règlement 2016/679 précité.

⁸² K. NDUKUMA ADJAYI (sous la dir.), A. DIANGENDA MVETE et B. LOLEKA RAMAZANI, *Droit du commerce électronique : enjeux civils, consommateurs, cyber-criminels, d'extranéité et de déterritorialité*, op.cit, p. 84.

58 - Le législateur français s'est inspiré ouvertement de la décision de la Cour constitutionnelle fédérale allemande du 15 décembre 1983, en complétant l'article 1^{er} alinéa 2 de la loi Informatique et libertés qui dispose que : « Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi ». Cet alinéa, qui ne figurait pas dans le texte initial, est issu de la loi n°2016-121 du 7 octobre 2016 pour une République numérique ». C'est ainsi que le droit à l'autodétermination informationnelle apparaît plus approprié à la défense du principe du principe de consentement individuel par rapport à ses données personnelles.⁸³

59 - Pratiquement, cette consécration du droit à l'autodétermination informationnelle avait été soutenue par le Conseil d'État français dans son rapport « numérique et droits fondamentaux » de 2014 en ces termes : « *alors que le droit à la protection des données [reconnu par la Charte des droits fondamentaux de l'Union européenne] peut-être perçu comme un concept défensif, le droit à l'autodétermination lui donne un contenu positif. Il ne s'agit plus seulement de protéger le droit au respect de la vie privée, mais d'affirmer la primauté de la personne qui doit être en mesure d'exercer sa liberté. En ce sens, le droit à l'autodétermination répond davantage à l'aspiration croissante des individus à l'autonomie de décision*⁸⁴ ».

60 - S'agissant du droit congolais, l'article 31 de la Constitution consacre le droit fondamental à la protection du secret de correspondance émise par voie de télécommunication ou de toute autre forme de communication, [y compris sur Internet].⁸⁵ Cette protection est renforcée tant par la loi n°20/017 du 25 novembre 2020 relative aux télécoms et aux TIC que par le code du numérique du 13 mars 2023. Ces deux textes consacrent non seulement le droit au secret des correspondances émises par voie de télécommunication et des TIC [...],⁸⁶ mais prévoient en outre que tout traitement des données à caractère personnel ne peut s'effectuer qu'avec le consentement préalable de la personne concernée par le traitement.⁸⁷ Le consentement préalable de l'utilisateur concerné est également requis pour toute opération de collecte, d'enregistrement, de traitement, de stockage et de transmission des données à caractère personnel.⁸⁸ Le bien-fondé de ce droit réside dans la protection des individus contre l'utilisation abusive de leurs données. Il est un pilier de la protection des droits fondamentaux des individus dans la société de l'information.

b. Les droits à l'oubli et à la mort numériques

– Le droit à l'oubli [numérique]

61 - Dans une large mesure, le droit offre la possibilité de demander la suppression de données personnelles nous concernant, si celles-ci ne sont plus justifiées par une finalité suffisamment légitime. Peut-on considérer que l'effacement ou la suppression de données sur les moteurs de

⁸³ K. NDUKUMA ADJAYI, « L'avenir du droit des données et du service public de la donnée en République Démocratique du Congo », Conférence donnée, *Digital Rights and inclusion Forum DRC*, Kinshasa, 22 avril 2022, p. 5.

⁸⁴ Conseil d'Etat, « Étude annuelle 2014 : le numérique et les droits fondamentaux », La documentation française, 2014, p. 268.

⁸⁵ Article 31, Constitution du 18 février 2006, préc.

⁸⁶ Article 126, al. 1, loi n° 20/017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc.

⁸⁷ Articles 131 al. 2, loi n° 20/017 du 25 novembre 2020, préc. et 192 et 193, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁸⁸ Articles 132 al. 1, loi n° 20/017 du 25 novembre 2020 relative aux télécoms et aux TIC, préc. et 192 et 193, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

recherche ou réseaux sociaux suffise à les faire disparaître d’Internet ? En effet, lorsque les images ou d’autres types de données personnelles sont publiées sur Internet, elles sont rapidement dupliquées sur de nombreux serveurs appartenant à des sites Internet ou hébergeurs distincts. Il devient alors difficile de s’assurer qu’elles ont été effectivement et exhaustivement retirées et que des copies ne figurent pas quelque part. C’est tout l’enjeu, presque impossible⁸⁹, du droit à l’oubli numérique. Ce droit consiste à faire disparaître les traces, sur de multiples serveurs, d’une photo compromettante, d’une donnée confidentielle publiée ou d’une réputation endommagée par la rumeur.

62 - Le « droit à l’oubli » est d’origine jurisprudentielle. Il fut ainsi consacré par la Cour de Justice de l’Union européenne en 2014 dans son arrêt *Google Spain*⁹⁰. La CJUE définit ce droit comme « *l’obligation, pour un moteur de recherche, 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* ». On distingue alors le déréférencement (suppression des recherches) et l’effacement (suppression directe des pages web).

63 - Ce droit à l’oubli numérique peut être appréhendé de deux manières. En premier lieu, par le biais de l’interdiction faite au responsable du traitement de conserver les données collectées au-delà du temps nécessaire au traitement.⁹¹ Les dispositions sur la conservation des données posent en effet une obligation de suppression qui permet la concrétisation de ce droit à l’oubli et qui passe ici par la destruction ou l’anonymisation des données. En second lieu, le droit à l’oubli peut être considéré comme une concrétisation du droit d’effacement des données en cause. Le titulaire des informations collectées est en droit de demander à ce qu’elles disparaissent des bases de données et pages Internet et ne soient plus référencées par les moteurs de recherche. On parle ici d’opérations de « désindexation » ou de « déréférencement ».⁹²

64 - Depuis l’entrée en vigueur du RGPD, les pays membres de l’Union européenne disposent d’une base juridique sur le droit à l’oubli. En effet, l’article 17 du RGPD offre 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.

65 - S’inspirant de cette disposition, le code du numérique congolais consacre ce droit à l’effacement en son article 215 équivalent de l’article 40 de loi Informatique et Libertés. Ainsi, le responsable du traitement a l’obligation d’effacer les données à caractère personnel dans le délai de 30 jours lorsque l’un des motifs suivants s’applique :

1. les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d’une autre manière ;
2. pour respecter une obligation légale à laquelle le responsable du traitement est soumis ;
3. pour exécuter une mission d’intérêt public [...] ;

⁸⁹ GUY DE FELCOURT, *op.cit.*, p. 120.

⁹⁰ CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12 : RLDI, août 2014, n° 107, p. 32.

⁹¹ Article 193. 3, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc. équivalent de l’article 6.5°, loi française de 6 janvier 1978, préc.

⁹² L. GRYNBAUM, C. LEGOFFIC et L. MORLET-HIDARA, *op.cit.*, p. 846.

4. les données à caractère personnel ont fait l'objet d'un traitement illicite ;
5. la personne concernée retire le consentement sur lequel est fondé le traitement [...].⁹³

66 - Cependant, le droit à l'oubli n'est pas ici considéré comme absolu, car les cas dans lesquels on peut le faire valoir sont limitativement énumérés. En outre, le droit à l'oubli ne doit pas compromettre d'autres droits existants. Comme bien souvent s'agissant des droits des individus dans le cadre de l'usage des réseaux numériques, un équilibre doit ici être trouvé entre la protection des données personnelles, la libre circulation de l'information, la nécessité de pouvoir se ménager des preuves, le devoir de mémoire et la liberté d'expression. C'est ainsi que l'article 216 alinéa 4 du code du numérique, équivalent de l'article 17 point 3 du RGPD fixe les motifs pour lesquels le droit à l'oubli ne pourra pas être accordé. C'est généralement lorsque le traitement est nécessaire :

1. à l'exercice du droit à la liberté d'expression et d'information ;
2. au respect d'une obligation légale [...]
3. à des motifs d'intérêt public dans le domaine de la santé publique ;
4. à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique [...]
5. à la constatation, à l'exercice ou à la défense de droits en justice.

67 - La consécration du droit à l'oubli depuis la décision de la CJUE de 2014 avait contraint le moteur de recherche Google à mettre en place un formulaire de droit à l'oubli.⁹⁴ Ce formulaire répond aux besoins de protéger la réputation des individus en ligne tout en leur permettant de contrôler, dans une certaine mesure, l'image qu'ils envoient sur internet. Pour aller plus loin, le législateur a consacré également le droit à la mort numérique.

– *Le droit à la mort [numérique]*

68 - Il sied de rappeler que le législateur congolais s'est également inspiré du droit français quant au sort réservé aux données identitaires d'un individu après sa mort. À cet effet, la loi française pour la République numérique avait consacré dès octobre 2016, le principe de l'énonciation de la « mort numérique » comme découlant de la liberté d'autodétermination informationnelle.⁹⁵ Ce droit consiste pour une personne de décider de ce que deviendraient ses données personnelles après sa mort, comme une sorte de testament.

69 - Sur le plan pratique, la quasi-totalité des Géants du numérique prévoient, à ce jour, la possibilité de désignation d'un contact légataire (*Legacy Contact*). Ce dernier est choisi par le titulaire d'un compte sur une plateforme numérique pour accéder à ses données numériques après sa mort. Cette procédure permet non seulement de préserver la mémoire du défunt sur les réseaux mais aussi de faciliter certaines démarches administratives en ligne (réseaux sociaux, *iCloud*, boîtes mails, etc.).

⁹³ Article 17.1, Règlement (UE) 2016/679, préc.

⁹⁴ Google, « Présentation du droit à l'oubli », [<https://support.google.com/legal/answer/10769224?hl=fr>]

⁹⁵ V. article 63, 3°, loi française n°2016-1321 du 7 octobre 2016 pour une République numérique.

70 - Dans la même optique, le code du numérique congolais fait obligation au responsable de traitement des données d'informer la personne concernée de la possibilité de définir les modalités de la gestion de ses données personnelles après sa mort⁹⁶ à défaut, ce sont les héritiers légaux qui sont en droit d'agir sur ces données. La consécration de ce droit par le code du numérique constitue une avancée majeure de notre législation en constante évolution. Les citoyens congolais ont désormais la possibilité de déterminer le sort de leurs données personnelles après la mort. Ce droit permet de préserver l'intimité du *de cuius* et protège son identité numérique en évitant la divulgation non consentie de ses données personnelles.

B. L'esquisse d'une identité digitale en RD Congo

71 - Face à la prolifération de menaces liées à l'usurpation d'identité en ligne, malgré l'arsenal pénal en vigueur, ajouté à cela des dégâts invisibles et difficilement quantifiables causés par la cybercriminalité, faute de mécanismes d'identification suffisamment fiable en ligne, certains pays ont adopté des solutions censées procurer à la fois un haut niveau de fiabilité, et un très large éventail d'utilisations en ligne.⁹⁷

72 - Les plateformes d'identification numériques diffèrent d'un pays à l'autre selon la technologie utilisée. L'Estonie et l'Inde sont deux exemples à l'opposé l'un de l'autre. Le Gouvernement estonien s'appuie sur un solide système d'état civil où il enregistre numériquement les données d'identité, et délivre une carte d'identité à puce. Le titulaire peut utiliser son identité numérique au moyen d'un numéro d'identification personnel (NIP). Aucun renseignement biométrique n'est recueilli. En revanche, le Gouvernement indien a instauré un système biométrique reposant sur la saisie des dix (10) empreintes digitales et de deux (2) iris de chaque individu enregistré auquel est attribué un numéro identifiant unique (NIU) à 12 chiffres.⁹⁸ Ce numéro d'identification peut être utilisé pour plusieurs services publics et privés en ligne.

73 - Au niveau européen, l'UE avait envisagé la mise en place d'un portefeuille numérique européen appelé « *EUDI wallet* ». Ce portefeuille est institué par le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique. Entrée en vigueur le 20 mai 2024, ce Règlement vise à assurer l'identification et l'authentification électroniques des individus et des entreprises de manière sécurisée et fiable dans toute l'UE à travers un portefeuille numérique. D'ici 2026, ce portefeuille permettra aux citoyens et résidents européens non seulement de prouver leur identité, de stocker et échanger les documents mais aussi d'avoir accès à une variété de services publics et privés, tant en ligne que hors ligne.⁹⁹ Dans tous les cas, les citoyens auront à tout moment le plein contrôle des données qu'ils partagent et des destinataires de ces données.¹⁰⁰

⁹⁶ Article 208, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

⁹⁷ E. NETTER, *Numérique et grandes notions du droit privé : la personne, la propriété, le contrat*, op.cit., p. 63.

⁹⁸ BANQUE MONDIALE, « Guide de l'identité électronique : À l'intention des parties prenantes d'Afrique », op.cit., p. 5.

⁹⁹ Commission européenne, « Identité numérique européenne » [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr], (consulté le 21 novembre 2024).

¹⁰⁰ Article 5 bis et sv, Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.

74 - Dans son programme « identification pour le développement (ID4D) », la Banque Mondiale avait déploré que : « *plus de 1,1 milliard de personnes, dont la moitié est en Afrique, sont incapables de prouver leur identité avec un document officiel.*¹⁰¹ Elles ont par conséquent, du mal à accéder aux services gouvernementaux et économiques essentiels, plus particulièrement aux services financiers, de santé, d'éducation, etc. » Les initiatives ID4D des Nations Unies et de la Banque Mondiale, se sont fixé pour objectif de donner une identité juridique à tous les habitants de la planète d'ici 2030.

75 - L'identification constitue un immense défi pour la RD Congo qui ne dispose pas, à ce jour, d'un système efficace lui permettant d'identifier l'ensemble de sa population. Cependant, on constate une fragmentation de la filière d'identification, caractérisée par une concurrence entre nombreux services de l'État. C'est le cas notamment de la carte d'électeur, du passeport, du casier judiciaire, de permis de conduire, de certificat de nationalité, de l'acte de naissance, etc.

76 - Bien que la RD Congo ne dispose pas [encore] d'un système d'identification efficace à ce jour, on remarque néanmoins une volonté dans le chef du Gouvernement de doter le pays d'un Système National d'Identification Digitale (SNID). Cette volonté s'était déjà manifestée par l'adoption en 2019, du Plan national du numérique horizon 2025 (PNN). Ce document de politique publique avait prévu dans son chronogramme des actions prioritaires, la réalisation d'un projet relatif à l'identification électronique de toute la population. Ce projet avait pour objectif d'instaurer pour chaque citoyen l'identifiant numérique unique dans le fichier général de la population et les autres fichiers documentaires.¹⁰² Par la suite, s'en était suivie l'adoption par le Conseil des Ministres du 31 janvier 2020, du projet de mise en place du SNID en RD Congo. À cette occasion, un Comité de Suivi réunissant plus de dix Ministères avait été mis en place pour mener à bon port ledit projet.

77 - C'est également dans ce cadre que la Banque Africaine de Développement (BAD) avait lancé un avis à manifestation d'intérêts pour recruter, selon la procédure d'appel d'offres standard, un Cabinet conseil devant conduire une étude de faisabilité du SNID en RD Congo. Et c'est le Cabinet Ernst & Young qui fut retenu.¹⁰³ D'après la BAD, les services prévus au titre de cette mission concernaient l'analyse de l'existant en matière d'identification des personnes, l'étude de faisabilité complète sur la mise en place d'un SNID, les actions d'accompagnement à mettre en œuvre.¹⁰⁴ Ce projet fut interrompu de manière inattendue, sans que les raisons de cette interruption de soient révélées.

¹⁰¹ Banque mondiale, « Accès pour tous à une identité numérique d'ici 2030 : les dirigeants africains, le Groupe de la Banque Mondiale et les partenaires se mobilisent », Communiqué de presse, 25 septembre 2018, in [https://www.banquemondiale.org/fr/news/press-release/2018/09/25/african-leaders-the-world-bank-group-and-partners-catalyze-action-to-ensure-that-everyone-in-africa-has-a-digital-identity-by-2030] (consulté le 12 février 2022).

¹⁰² Présidence de la République, « Plan national du numérique Horizon 2025 », Kinshasa, septembre 2019, p. 56.

¹⁰³ Cabinet du Numérique (RDC), « Registre national : la carte d'identité biométrique bientôt une réalité en RDC », 10 novembre 2020, in [https://www.numérique.cd/fr/2020/11/registre-national-la-carte-didentite-biometrique-bientot-une-realite-en-rdc/] (consulté le 12 février 2022).

¹⁰⁴ DBA, « RD Congo : Recruté par la BAD, Ernst & Young va réaliser l'étude de faisabilité de la mise en œuvre d'un système national d'identité digitale », 13 novembre 2020, disponible sur : [https://www.google.com/amp/s/www.digitalbusiness.africa/rd-congo-recrute-par-la-bad-ernst-young-va-realiser-letude-de-faisabilite-de-la-mise-en-place-dun-systeme-national-didentite-digitale/%3famp] (consulté le 12 février 2022).

78 - Pour concrétiser le projet d'identification de la population, le Premier Ministre avait signé, en date du 2 mars 2022, une série de décrets visant à offrir aux Congolais une identité fiable, à savoir :

- le Décret n°22/07 du 02 mars 2022 portant création d'un fichier général de la population en République Démocratique du Congo (FGP). Le FGP est un système de traitement des données individualisées qui contient les informations biographiques et biométriques relatives à l'identité des personnes physiques et celles relatives à l'état civil.¹⁰⁵ Ainsi, un numéro d'identification nationale sera attribué à chaque personne physique lors de son premier enregistrement au FGP¹⁰⁶ ;
- le Décret n°22/08 du 02 mars 2022 portant création d'une carte d'identité nationale en République Démocratique du Congo. Ce décret crée un titre d'identité pour citoyen congolais, dénommé « Carte d'Identité Nationale (CIN) ». ¹⁰⁷ La CIN certifie et fixe l'identité congolaise de son titulaire.¹⁰⁸ Elle est délivrée par l'Office National de la Population à tout Congolais vivant sur le territoire national ou à l'étranger. La CIN qui a une validité de dix ans renouvelable¹⁰⁹ contient des informations à caractère personnel, les unes visibles à l'œil nu et les autres lisibles de manière électronique ou numérique.¹¹⁰ La procédure de demande, le coût et les conditions d'obtention et de renouvellement seront fixés par un arrêté du ministre de l'Intérieur¹¹¹ ;
- le Décret n°22/09 du 02 mars 2022 portant organisation de la mutualisation des activités opérationnelles dans le cadre de l'identification et de l'enrôlement des électeurs, de l'identification de la population et du recensement général de la population et l'habitat. La mutualisation opérationnelle consiste en la mise en commun des ressources humaines, techniques, logistiques et matérielles dédiées à la réalisation des activités communes, en vue de contribuer à la production des cartographies opérationnelles, du fichier électoral et du fichier de général de la population.¹¹² Cette mutualisation opérationnelle est assurée par un comité de pilotage et un comité technique.¹¹³

79 - Cependant, en vue de la production des cartes d'identités nationales et la gestion du fichier général de la population, l'Office Nationale de l'identification de population(ONIP) avait signé un contrat d'une durée de 20 ans avec le consortium IDEMIA/AFRITECH pour plus d'un milliard de dollars soit 697 millions de dollars à titre d'apport de l'État congolais, et 503 millions de dollars du consortium.¹¹⁴

80 - En termes de caractéristiques, cette nouvelle carte biométrique était faite de matériaux durables pour résister aux intempéries pour une durée de dix ans. Elle possédait une puce sans

¹⁰⁵ Article 2, Décret n°22/07 du 02 mars 2022 portant création d'un fichier général de la population en République Démocratique du Congo.

¹⁰⁶ Article 8, Décret n°22/07 du 02 mars 2022, préc.

¹⁰⁷ Article 1^{er}, Décret n°22/08 du 02 mars 2022 portant création d'une carte d'identité nationale en RDC, préc.

¹⁰⁸ *Ibid.*

¹⁰⁹ Article 3, Décret n°22/08 du 02 mars 2022, préc.

¹¹⁰ Article 4, Décret n°22/08 du 02 mars 2022, préc.

¹¹¹ Article 7, Décret n°22/08 du 02 mars 2022, préc.

¹¹² Article 1^{er}, Décret n°22/09 du 02 mars 2022, préc.

¹¹³ Article 4, Décret n°22/09 du 02 mars 2022, préc.

¹¹⁴ CH. OUSMAN MBARDOUNKA, « Le pays africain dont les citoyens n'ont pas de carte d'identité depuis 40 ans », 14 mai 2024, BBC Afrique, disponible sur : <https://www.bbc.com/afrique/articles/cy633p6ezq1o> (consulté le 21 septembre 2024).

contact qui permet entre autres l'authentification du porteur. La puce, le système d'exploitation et l'applet étaient conformes à la norme ICAO (International Civil Aviation Organisation).

81 - C'est finalement en date du 30 juin 2023 que l'ONIP avait délivré la première carte d'identité nationale au Président de la République en tant que Premier citoyen de la République. Près d'un an plus tard, soit le 26 avril 2024, l'ONIP devrait procéder à la reprise effective des opérations de délivrance de la carte d'identité dans les communes pilotes de Kinshasa.¹¹⁵ Mais fort malheureusement, le contrat a été résilié par consentement mutuel des parties en date du 12 août 2024, à la suite des irrégularités constatées.¹¹⁶

82 - À ce jour, les trois décrets du 2 mars 2022 précités sont supplantés par le code du numérique du 13 mars 2023 et devraient, en toute logique, être revus pour intégrer les aspects liés à l'identification électronique consacrée par ledit code. L'identification électronique désigne un processus qui consiste à l'utilisation des données et éléments constitutifs de l'identité d'une personne physique ou morale par des procédés électroniques qui représentent de manière univoque la personne physique ou morale concernée.¹¹⁷

83 - Le code du numérique a ainsi prévu que l'État, procède, au moyen d'identification électronique, à l'identification générale de la population et délivre une carte d'identité nationale à identifiant unique aux nationaux.¹¹⁸ Ce processus doit reposer sur un schéma électronique fiable devant déterminer les spécifications des niveaux de garantie faible, substantiel et/ou élevé des moyens d'identification électronique.¹¹⁹

84 - En termes d'obligations liées au moyen d'identification électronique, son titulaire est tenu de prendre toutes les dispositions possibles pour le garder sous son contrôle exclusif afin de prévenir le vol, la perte ou la divulgation. Si une telle situation arrive, le titulaire doit révoquer immédiatement le moyen d'identification électronique.¹²⁰

85 - Pour l'application effective du code du numérique en cette matière, il est prévu la signature d'un Décret par le Premier Ministre censé déterminer les éléments, les spécifications techniques des moyens d'identification électronique, les schémas d'identification électronique et leurs niveaux de garantie certifiant l'identification ainsi que le cadre d'interopérabilité.¹²¹ La signature de ce Décret marquera une étape considérable dans la modernisation de l'administration à l'ère du tout numérique. Elle ouvrira en outre, la voie à de nombreuses améliorations dans différents domaines de la vie sociale et économique des citoyens.

¹¹⁵ *Ibidem*.

¹¹⁶ Radio okapi, « La RDC rompt le contrat de production des cartes d'identité biométriques », 04/09/2024, disponible sur : [https://www.radio-okapi.net/2024/09/05/actualite/societe/la-rdc-rompt-le-contrat-de-production-des-cartes-didentite-biometriques] (consulté le 21 septembre 2024).

¹¹⁷ Articles 2 point 42 et 171, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

¹¹⁸ Article 172, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

¹¹⁹ Articles 174 à 181, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

¹²⁰ Article 182, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

¹²¹ Article 173, Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, préc.

CONCLUSION

86 - L'identité numérique cohabite avec la notion d'état civil dont elle constitue le socle. Elle représente beaucoup plus qu'une simple évolution des techniques d'identification, d'authentification et de signature en ligne. Elle a pour vocation de s'imposer dans les mondes physique et numérique, comme le moyen privilégié de reconnaissance de notre identité. Elle vient ajouter un nouvel usage des données sur les réseaux numériques, qui bouleversent notre mode de vie et transforment les modèles économiques.

87 - L'identification [numérique] est nécessaire tant pour la société prise globalement, que pour l'État, les administrations, les collectivités locales qui ont grand intérêt à connaître leurs citoyens, les électeurs, les contribuables, et toutes sortes de groupes dont le dénombrement est nécessaire à la politique économique et sociale de la nation. Elle favorise la prestation de services par voie électronique, ce qui décuple l'efficacité des pouvoirs publics et contribue à la création de nombreux produits et services en ligne. D'où la nécessité pour l'État [congolais] de se doter d'un système fiable et efficace d'identification de sa population.

88 - L'identification des personnes est donc un prérequis du développement moderne. Un solide système d'identification permettra à l'État (congolais) de saisir l'identité propre de chaque individu dans un fichier général de la population. Une fois ce fichier créé, les pouvoirs publics pourront attribuer à chaque personne une identité officielle, attestée par une carte nationale d'identité portant un numéro d'identifiant unique. L'application effective du code du numérique et ses mesures d'application s'avère urgente. Le décret portant création du Fichier général de la population et celui instituant la carte d'identité nationale ayant connu une application lente doivent se conformer au code du numérique. De plus, le Décret du Premier Ministre censé mettre en mouvement l'opération d'identification électronique se fait toujours attendre à l'heure où nous écrivons...

BIBLIOGRAPHIE INDICATIVE

I. TEXTE CONSTITUTIONNEL

- Constitution de la République Démocratique du Congo, modifiée par la loi no 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République Démocratique du Congo du 18 février 2006, in JO RDC, 52^e année, n° spécial, du 05 février 2011.

II. LÉGISLATION CONGOLAISE

1) Codes des lois et textes législatifs

- Loi n°16/008 du 15 juillet 2016 complétant et modifiant la loi n°87-010 du 1^{er} août 1987 portant code de la famille, in JO RDC, n° spécial.
- Loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication in JO RDC, 62^e année, n° spécial, du 22 septembre 2021.
- Décret du 30 janvier 1940 tel que modifié, complété et mis à jour au 05 octobre 2006, portant Code pénal, in JO RDC, 47^e année, n° spécial, du 05 octobre 2006.
- Ordonnance-loi n°23/010 du 13 mars 2023 portant code du numérique, JO RDC, numéro spécial, 64^e année, 11 avril 2023.

2) Textes réglementaires

- Décret n°22/07 du 02 mars 2022 portant création d'un fichier général de la population en République Démocratique du Congo (FGP).
- Décret n°22/08 du 02 mars 2022 portant création d'une carte d'identité nationale en République Démocratique du Congo.
- Décret n°22/09 du 02 mars 2022 portant organisation de la mutualisation des activités opérationnelles dans le cadre de l'identification et de l'enrôlement des électeurs, de l'identification de la population et du recensement général de la population et l'habitat.

II. LÉGISLATION EUROPÉENNE

- Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000.
- Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

III. LÉGISLATION AFRICAINE

- Convention de Malabo du 27 juin 2014 sur la cybersécurité et la protection des données à caractère personnel.

IV. LÉGISLATION FRANÇAISE

Code pénal français.

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO RF, 7 janvier 1978
- Loi n°2016-1321 du 7 octobre 2016 pour une République numérique, JO RF, 8 octobre 2016
- Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JO FR n°69, 23 mars 2011, dite « LOPSI II »

V. OUVRAGES

- Ameli F., *Droit : introduction, les personnes, les biens*, Montchretien, Paris, 2000.
- Amisi Herady, *Droit civil : les personnes, les incapacités, la famille*, Vol.1, 4^e éd., EDUPC, Kinshasa, 2016.
- Catala P., « Ébauche d'une théorie juridique de l'information », Dalloz, 1994.
- Cornu G., *Vocabulaire juridique*, 12^e éd, PUF Quadrige, Paris, 2018.
- Eynard J. (sous la dir.), *L'identité numérique : quelle définition pour quelle protection ?*, Larcier, Paris, 2020.
- Eynard J., *Les données personnelles : quelle définition pour un régime de protection ?*, Michalon, Coll. Essai, Paris, 2013.
- Grynbaum L., Legoffic C. et Morlet-Hidara L., *Précis de Droit des activités numériques*, 1^{ère} éd., Dalloz, Paris, 2014.
- Guinchard S. et Debard T., *Lexique des termes juridiques*, 25^e éd., Dalloz, Paris, 2017-2018.
- Guy De Felcourt, *L'usurpation d'identité ou l'art de la fraude sur les données personnelles*, Paris, CNRS Edition, 2011.
- Kaufmann J.C., *L'invention de soi, une théorie de l'identité*, Hachette littératures, Paris, 2004.
- Ndukuma Adjayi K. (sous la dir.), Diangenda Mvete A. et Loleka Ramazani B., *Droit du commerce électronique : enjeux civils, consommateurs, cybercriminels, d'extranéité et de déteritorialité*, L'Harmattan, coll. « Enjeux et droits numériques », Paris, 2021.
- Ndukuma Adjayi K., *Droits des télécoms et du numérique : Profil africain et congolais, prospective comparée d'Europe et de France*, tome II, Paris, l'Harmattan, 2019.
- Terre F., *Introduction générale au droit*, 4^e éd., Dalloz, Paris, 1998.
- Zenati-Castaing F. et Revet T., *Manuel de droit des personnes*, PUF, Coll. Droit Fondamental, Paris, 2006.

VI. ARTICLES

1) Articles généraux

- Boucher P., « Safari ou la chasse aux Français », in *Le monde*, 21 mars 1974.
- Caprioli É., « De l'usurpation d'identité en matière pénale », sous *Crim.* 29 mars 2006, n° 05-

85.857 : Bull. crim. n° 94 ; CCE n° 7, juill. 2006, comm. 117.

- Georges F., « L'Approche statistique de trois composantes de l'identité numérique dans Facebook », in F. Millerand, S. Proulx, J. Rueff (sous la dir.), *Web social : Mutation de la communication*, PUQ, Québec, 2010.
- Lacroix C., « Rép. Pén », Dalloz, juin 2012, V° usurpation d'identité, n°1.

2) Articles accessibles en ligne

- Coëffé Th., « Qu'est-ce que l'identité numérique ? », in Regionsjob, 08 décembre 2014 - Mis à jour le 17 novembre 2015, disponible sur : [<https://www.regionsjob.com/conseils/identite-numerique-definition.html>] (consulté le 11 janvier 2022).
- Georges F., « L'identité numérique sous emprise culturelle : De l'expression de soi à sa standardisation » in *Les Cahiers du numérique* 2011/1, Vol. 7, pp. 3-48. Disponible sur : [<https://www.cairn.info/revue-les-cahiers-du-numerique-2011-1-page-31.htm>] (consulté le 11 janvier 2022).
- Kandolo Brozeck, « Régulation du numérique en RDC : l'ARPTIC investie Autorité unique pour la régulation du numérique, la certification électronique et la protection des données », Dossier n°4, in *Droit-Numérique.cd*, octobre 2024, disponible sur : [<https://droitnumerique.cd/regulation-du-numerique-en-rdc-larptic-investie-autorite-unique-pour-la-regulation-du-numerique-la-certification-electronique-et-la-protection-des-donnees/>], (consulté le 23 octobre 2024).

VII. THÈSES ET MÉMOIRES

- Dufour Baidouri A., *L'identité numérique : un levier d'innovation pour les marques ?*, Thèse de doctorat en Science de l'Information et de la Communication présentée et soutenue publiquement le 4 décembre 2013, Université Panthéon Assas, sous la dir. Prof. Francis Balle, Paris, 2013.
- Netter E., *Numérique et grandes notions du droit privé : la personne, la propriété, le contrat*, Mémoire en vue de l'habilitation à diriger des recherches en droit privé, présenté et soutenu publiquement le 20 novembre 2017, Garante : Judith Rochfeld, Université de Picardie - Jules Verne, 2017.
- Stella É., *L'adaptation du droit pénal aux réseaux sociaux en ligne*, Thèse en vue de l'obtention du grade de Docteur en droit privé et sciences criminelles présentée et soutenue publiquement le 12 décembre 2019, sous la dir. Frédéric Stasiak, Université de Lorraine, Lorraine, 2019.

VIII. AUTRES DOCUMENTS

- Banque Mondiale, « Accès pour tous à une identité numérique d'ici 2030 : les dirigeants africains, le Groupe de la Banque Mondiale et les partenaires se mobilisent », Communiqué de presse, 25 septembre 2018, in [<https://www.banquemondiale.org/fr/news/press-release/2018/09/25/african-leaders-the-world-bank-group-and-partners-catalyze-action-to-ensure-that-everyone-in-africa-has>

a-digital-identity-by-2030] (consulté le 12 février 2022).

- Banque Mondiale, « Guide de l'identité électronique : À l'intention des parties prenantes d'Afrique », juin 2014.
- Cabinet du Numérique, « Registre national : la carte d'identité biométrique bientôt une réalité en RDC », 10 novembre 2020, in [<https://www.numerique.cd/fr/2020/11/registre-national-la-carte-didentite-biometrique-bientot-une-realite-en-rdc/>] (consulté le 12 février 2022).
- Conseil d'État, « Étude annuelle 2014 : le numérique et les droits fondamentaux », La documentation française, 2014.
- DBA, « RD Congo : Recruté par la BAD, Ernst & Young va réaliser l'étude de faisabilité de la mise en œuvre d'un système national d'identité digitale », 13 novembre 2020, disponible sur : [<https://www.google.com/amp/s/www.digitalbusiness.africa/rd-congo-recrute-par-la-bad-ernst-young-va-realiser-letude-de-faisabilite-de-la-mise-en-place-dun-systeme-national-didentite-digitale/%3famp>] (consulté le 12 février 2022).
- Ndukuma Adjayi K., « L'avenir du droit des données et du service public de la donnée en République Démocratique du Congo », Conférence donnée, *Digital Rights and inclusion Forum DRC*, Kinshasa, 22 avril 2022.
- OCDE, « Document exploratoire sur le vol d'identité en ligne », juin 2008, p. 5. Disponible sur : [<https://www.oecd.org.stiPDF>], (consulté le 17 janvier 2022).
- Présidence de la République, « Plan national du numérique Horizon 2025 », Kinshasa, septembre 2019.



Droit-Numérique.cd est un cadre d'études dédié à l'analyse, la réflexion et la diffusion des connaissances juridiques relatives aux enjeux du numérique en **République démocratique du Congo**. Nous sommes enregistrés sous le numéro SIREN 931152144.

Pourquoi nous contacter ?

Partenariats

Collaborons pour renforcer l'écosystème numérique en RDC.

Consultations juridiques

Obtenez des conseils sur les questions légales liées au numérique.

Participation

Nous pouvons contribuer dans vos études, séminaires, et autres activités.

Suggestions

Partagez vos idées ou proposez des sujets que vous aimeriez voir abordés



 contact@droitnumerique.cd

 + 33 6 05 50 17 84

 www.droitnumerique.cd 

