

La protection de l'identité numérique du salarié en droit congolais : entre surveillance légitime et vie privée

Joël LUTAKU WATA

Juriste

MOTS-CLÉS

Identité civile
Identité numérique
Données personnelles
Relations de travail
Surveillance numérique
Profilage
Vie privée

RÉSUMÉ

Le numérique reconfigure silencieusement les architectures du droit de l'identité. La RD Congo se trouve saisie dans un mouvement de dédoublement critique, oscillant entre la précarité d'un état civil défaillant et l'hypertrophie d'une identité numérique envahissante. La première, fragilisée par les carences structurelles de l'enregistrement administratif, ne parvient plus à garantir l'univocité juridique de la personne, tandis que la seconde, proliférante et disséminée, recompose l'individu en un agrégat de traces en ligne exploitables. Dans les relations du travail, l'employeur est un responsable de traitement des données du salarié. Le recours généralisé à la vidéosurveillance et à la géolocalisation institue un régime de surveillance continue, transformant le lien de subordination en une emprise diffuse. Le lien de subordination se mue en contrôle algorithmique. Les principes de protection des données des salariés sont souvent détournés. L'identité numérique devient outil de profilage et de discrimination. Le cadre juridique reste formel mais inefficace. Dans la pratique professionnelle en RD Congo, il s'impose une domination capitaliste de l'employeur, au détriment de la vie privée et de la dignité du salarié.

Keywords :

Civil identity
Digital identity
Personal data
Labor relations
Digital surveillance
Profiling
Privacy.

ABSTRACT :

Digital technology is silently reshaping the architectures of identity law. The DRC is caught in a movement of critical doubling, oscillating between the precariousness of a failing civil status and the hypertrophy of an invasive digital identity. The former, weakened by the structural deficiencies of administrative registration, can no longer guarantee the legal univocity of the person, while the latter, proliferating and disseminated, recomposes the individual into an aggregate of exploitable online traces. In labor relations, the employer is a data controller of the employee's data. The widespread use of video surveillance and geolocation establishes a regime of continuous monitoring, transforming the subordinate relationship into a diffuse control. The subordinate relationship turns into algorithmic control. The principles of employee data protection are often misused. Digital identity becomes a tool for profiling and discrimination. The legal framework remains formal but ineffective. In professional practice in the DR Congo, capitalist domination of the employer imposes itself, to the detriment of employee privacy and dignity.

PROLÉGOMÈNES

La loi n° 87/010 du 1er août 1987 portant Code de la famille ancre l'identité dans l'état civil. Il est de principe que tout individu né vivant et viable y est déclaré dans un délai de trois mois¹. Mais, en réalité, de nombreux congolais naissent sans enregistrement officiel, dans un contexte marqué par une dynamique démographique soutenue. Les mécanismes administratifs peinent ainsi à épouser les réalités du terrain². Il en résulte une fragilisation de la fiabilité de l'identification civile des citoyens congolais. S'ensuivent, de manière corrélative, des risques accrus de falsification et/ou d'usurpation d'identité³.

À l'ère du numérique, la théorie des technologies de soi s'avère particulièrement éclairante pour comprendre la redéfinition de l'identité en RD. Congo⁴. Au fur et à mesure, les internautes congolais investissent leurs données personnelles dans les réseaux sociaux numériques. Ce qui fait que, de nos jours, la RD. Congo compte plus de 68 millions de connexions mobiles et près de 40 à 45 millions d'internautes.⁵ Ces données statistiques représentent un taux de pénétration d'environ

¹ Article 116, Loi n° 87/010 du 1er août 1987 portant code de la famille telle que modifiée par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er août 1987, in J.O RDC, 15 juillet 2016.

² R. POURTIER, « la République démocratique du Congo face au défi démographique », *Institut Français des relations Internationales, L'Ifri*, septembre 2018, p. 1

³ Article 69, loi n° 87/010 du 1er août 1987 portant code de la famille telle que modifiée par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er août 1987, préc.

⁴ Les technologies de soi désignent l'ensemble des pratiques par lesquelles les individus agissent sur eux-mêmes afin de se constituer en tant que sujets. Appliquée aux environnements numériques, cette grille d'analyse permet de comprendre comment les individus participent activement à l'auto-construction de leur identité à travers des dispositifs techniques tels que les réseaux sociaux ou les profils en ligne. V. J. REVEL, « Michel Foucault : repenser la technique », Dans *revue des Sciences Humaines*, n° 16, 2009, pp. 139-149

⁵ Autorité de Régulation de la Poste et des Télécommunications du Congo ARPTC, « observatoire du marché de la téléphonie mobile », rapport du 1er trimestre 2024.

40 % à 57 % de la population. Ce taux grandissant de pénétration des TIC⁶ et de l'internet généralisé change les représentations de la présence⁷.

En RD. Congo, l'identité numérique n'est pas sans incidence sur les rapports sociaux. Elle trouve un terrain d'expression dans les relations de travail. L'identification du salarié ne relève plus seulement de données civiles. Elle s'étend désormais à un ensemble de traces numériques⁸, susceptibles d'influencer tant l'accès à l'emploi que les conditions de son exercice.

Dès la phase de recrutement, les profils en ligne des candidats sont très souvent consultés par les employeurs. L'identité numérique devient une sorte de critère d'évaluation implicite. Elle peut faciliter l'embauche lorsqu'elle ne présente pas une mauvaise réputation en ligne. Dans certains cas, l'identité numérique devient une cause de stigmatisation de l'accès à l'emploi aux jeunes. La prolifération des diffusions des sextapes en moyenne 10 par semaine à Kinshasa produit des effets lourds sur des victimes en RD. Congo⁹.

Pendant l'exécution du contrat de travail, ces pratiques de contrôle persistent. Elles s'intensifient sous l'effet de la surveillance technologique du salarié¹⁰, justifiée par le lien de subordination¹¹. La plupart des entreprises basées à Kinshasa filme et stocke les images de chaque fait et geste des salariés. Le salarié ignore pendant combien de temps ces données sont stockées et leurs finalités exactes. Cette situation favorise certains abus. L'employeur, en tant que responsable de traitement, peut exploiter ou conserver des données au-delà des finalités strictement professionnelles. Les sous-traitants, notamment les banques chargées du paiement des salaires, participent aussi à la circulation et au traitement de ces données.

Après l'exécution du contrat de travail, l'identité numérique du salarié continue de produire des effets concrets. Le salarié conserve souvent une faible connaissance de ses droits relatifs à ses données personnelles et professionnelles et des limites dans le traitement. Cette méconnaissance limite sa capacité à contrôler l'usage, la conservation ou la diffusion de ses informations par l'employeur.

L'identité numérique du salarié se révèle ainsi un enjeu majeur, à la fois juridique, économique et social, exposant les individus à des risques de surveillance, de discrimination et d'usurpation, depuis le recrutement jusqu'au suivi post-contrat de travail.

Face à cet état des choses, on se pose la question suivante : Comment l'identité numérique reconfigure-t-elle les relations de travail en RD Congo, et quels enjeux juridiques, socio-culturels et institutionnels en découlent ?

⁶ L'acronyme NTIC (ou « TIC » équivalent de l'anglais ICT : « information and communication technologies ») désigne l'ensemble des technologies permettant de traiter des informations numériques et de les transmettre.

⁷ D. PERAYA, « Les changements induits par les technologies », in *Actes du Colloque CETSIS-EEA 1999*, Montpellier, université de Montpellier II, Cépaduès, 4 et 5 novembre 1999, p.185-188.

⁸ Antoinette Rouvroy théorise la manière dont les Big Data et les algorithmes exploitent ces traces numériques. Ce n'est plus la représentation de l'individu qui compte, mais le traitement de ses données comportementales. Les individus sont segmentés et dilués en profils numériques (profilage), créant une forme de surveillance qui anticipe les comportements plutôt que de surveiller les actions réelles. Le fétichisme des données prétend accéder au réel sans interprétation humaine. Elle montre comment les traces numériques ne forment pas une personne, mais un agrégat de potentialités sur lesquelles le sujet n'a plus de prise.

⁹ - l'affaire Eliane Bafeno contre le Pasteur Moïse Mbiye ; le cas de l'étudiante congolaise Édith NTAMBWA KINKELA de G2 Médecine, UPC ; le cas de Monsieur. Amisi Makutano, Président du Conseil d'Administration de l'OGEFREM et cadre au sein du parti présidentiel, etc.

¹⁰ Voir SHOSHANA ZUBOFF, *L'Âge du capitalisme de surveillance*, traduit de l'anglais par B. FORMENTELLI et A. S. HOMASSEL, éd. Zulma, Paris, 2020. En RD Congo, et notamment dans les entreprises implantées à Kinshasa, cette situation se matérialise par le recours croissant à des outils concrets tels que la vidéosurveillance permanente, les systèmes de contrôle d'accès électroniques, la traçabilité numérique des activités (*badges, logiciels de suivi*), voire, dans certains cas, des dispositifs de monitoring informatique. Ces technologies permettent une captation continue des comportements des salariés, transformant ainsi l'espace de travail en un environnement potentiellement hyper-surveillé. Toutefois, l'un des enjeux majeurs réside dans l'opacité qui entoure ces dispositifs. Les salariés ignorent fréquemment la durée de conservation des données collectées, leurs finalités exactes, ainsi que les modalités de leur traitement. Cette absence de transparence soulève des interrogations sérieuses au regard du respect de la vie privée et de la protection des données personnelles des salariés.

¹¹ Le lien de subordination est le critère fondamental du contrat de travail, défini à l'article 7, alinéa C du Code du travail congolais. Il se caractérise par l'exécution d'un travail sous la direction et l'autorité de l'employeur (ordres, contrôle, sanctions).

C'est autour de cette question que s'articulent nos axes de réflexion, auxquels les lignes suivantes apportent des réponses exploratoires.

L'identité numérique se superposerait à l'identité civile en RD Congo. Ceci expose le salarié à des atteintes potentielles aux données professionnelles du salarié congolais.

En RD Congo, la protection des données des salariés resterait limitée tant que l'APD n'est pas encore opérationnelle. Les compétences provisoires de l'ARPTIC dans la protection des données deviennent une sorte de surcharge pour cet établissement public. La conformité des employeurs dans le traitement des données des salariés serait incertaine et inexistante. Il y a un écart entre les exigences légales et la réalité des pratiques professionnelles, qui renforcent la vulnérabilité presque consentie des salariés.

L'exercice des droits des salariés en matière de protection des données serait encore fragmentaire, particulièrement dans les PME peu sensibilisées. Le traitement des données des salariés ne devrait rester strictement limité aux finalités légitimes liées au contrat de travail. Il est nécessaire de concilier la vie privée du salarié avec les exigences organisationnelles en milieu professionnel. Les groupes syndicaux devraient négocier des conventions collectives en matière de protection des données des salariés en RD Congo. La désignation d'un Délégué à la protection des données dans chaque entreprise renforcerait concrètement la garantie des droits des salariés.

L'analyse de l'identité numérique sur les relations de travail en RD Congo nous exige une démarche méthodologique d'analyse juridique comparative et empirique. Nous analysons les textes juridiques internationaux, nationaux et étrangers sur l'identité numérique dans les relations de travail. Nous examinons la réalité socio-culturelle congolaise à travers une approche empirique. Nous observons la manière dont les employeurs perçoivent et protègent l'identité numérique des salariés.

Cette étude déploie sa réflexion autour de deux dimensions. La première, centrée sur le passage de l'identité civile à son expression numérique (I), et la seconde, consacrée aux implications et retombées de cette mutation dans les relations de travail en RD Congo (II).

I. DE L'IDENTITÉ CIVILE À L'IDENTITÉ NUMÉRIQUE ■

L'identité classique est ancrée dans les registres d'état civil. Elle s'étend désormais dans une dynamique élargie dans les usages numériques. Pour s'en convaincre, il convient d'adopter un regard synchronique sur l'identité en droit civil congolais (I.1) afin d'en dégager les fondements. Puis, étendre la description de l'identité numérique (I.2), à ses mécanismes et à ses effets contemporains.

I.1. Identité en droit civil congolais

L'identité est, au sens classique du droit civil, l'ensemble d'éléments qui permettent d'attester qu'une personne correspond bien à celle qu'elle affirme être ou que la société reconnaît comme telle¹². Pour notre part, l'identité est l'ensemble des éléments fiables. Ils permettent d'établir la correspondance entre une personne réelle et celle qu'elle déclare être.

Cette approche repose implicitement sur un postulat de fiabilité et d'exhaustivité des mécanismes d'identification civile. Or, en RD Congo, ce postulat est largement mis en échec par les dysfonctionnements structurels de l'état civil¹³. L'identité civile est le reflet de toute personne dans

¹² S. GUINCHARD, T. DEBARD et al, *lexique des termes juridiques*, éd. Dalloz, Paris, 2017, p. 1082.

¹³ En application de la loi n° 87/010 du 1er août 1987 portant code de la famille telle que modifiée par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er août 1987, le décret n° 22/ 008 du 02 mars 2022 institue la Carte d'identité nationale comme pièce d'identification des citoyens congolais majeurs. La définition classique selon laquelle « l'identité est l'ensemble des éléments permettant d'attester qu'une personne correspond bien à celle qu'elle affirme être » appelle, au regard de la réalité congolaise, une relativisation critique importante. D'une part, une proportion significative de la population ne dispose pas d'une identité juridique formellement établie. Le taux d'enregistrement des naissances demeure particulièrement faible, avoisinant seulement 40 % au niveau national, avec des disparités encore plus marquées dans certaines provinces. D'autre part, même lorsque

sa relation avec l'État et avec autrui¹⁴. Elle est le socle sur lequel se greffent les droits et les obligations d'une personne. Elle décrit l'état de la personne qui est un ensemble des qualités auxquelles la loi attache des effets juridiques.¹⁵

Toutefois, en RD Congo, les données d'état civil sont souvent conservées de manière précaire. À Kinshasa, ces bureaux de l'état civil existent mais travaillent avec des difficultés matérielles remarquables. Ainsi, la définition proposée apparaît excessivement normative et déconnectée des réalités empiriques congolaises. Actuellement, l'identité civile est socialement et institutionnellement construite. Sa fiabilité dépend étroitement de l'effectivité des systèmes d'enregistrement.

L'identité civile revêt une valeur normative en ce qu'elle démontre la singularité de la personne. Elle constitue le creuset dans lequel se construisent la dignité et la liberté en assurant à chacun une existence stable et protégée¹⁶. À ce titre, elle entretient un lien étroit avec la vie privée¹⁷, dont elle délimite le périmètre. En effet, la vie privée se veut un espace dans lequel la personne se définit librement, à l'abri des ingérences¹⁸.

I.2. Extension vers l'identité numérique

L'identité numérique est comme un récit que chaque individu construit à travers des traces de ses activités en ligne¹⁹. Elle se forme par une fragmentation structurelle qui s'inscrit dans la logique de dividualité²⁰. Elle ne forme pas une unité cohérente, mais procède d'un agrégat de traces disséminées sur diverses plateformes numériques. L'individu y apparaît éclaté en données divisibles²¹ partiellement maîtrisées. Dès lors, le salarié n'est pas une entité juridique unifiée. Il devient une construction numérique mouvante, juridiquement difficile à saisir dans son intégralité.

En ce sens, l'identité numérique est un ensemble d'informations et un agrégat de traces ou sédiments des interactions de l'internaute avec le système informatique²². Pour notre part, l'identité numérique est donc l'ensemble d'informations, des traces et des interactions d'un individu en ligne. Elle permet d'identifier une personne de manière directe ou indirecte.

L'identité numérique se décline en trois types des traces numériques. La première catégorie regorge les informations partagées par l'individu lui-même. C'est l'identité numérique déclarative.

des mécanismes d'identification existent, leur fiabilité est contestée. Le système d'état civil congolais souffre de lacunes organisationnelles majeures : absence de registres fiables, destruction d'archives, insuffisance des infrastructures administratives et difficultés d'accès aux services publics.

¹⁴ Le besoin de l'identification des personnes se justifie à la fois pour les individus entre eux (Le besoin de l'identification entre les personnes renvoie au fait que l'on songe à la signature d'un contrat.) et dans les rapports avec l'État¹⁴ (Un besoin est de savoir où est domicilié la personne pour des besoins fiscaux). v. J.M. BRUGUIÈRE et B. GLEIZE, *Droit des personnes*, éd. Dalloz, Paris, 2023, p. 85.

¹⁵ R. SAVATIER, *traité pratique de droit civil français*, éd. LGDJ, Paris, 1952, p.13.

¹⁶ E. MILLARD, « Le rôle de l'état civil dans la construction de l'Etat », in *Centre de Théorie et Analyse du Droit*, n° 7074, p. 3. Le droit civil congolais protège cette identité en punissant son usurpation (Article 69, loi n° 87/010 du 1er aout 1987 portant code de la famille telle que modifié par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er aout 1987, préc. et article 351, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique en République Démocratique du Congo, préc.), en garantissant le respect de la vie privée (Article 31, Constitution de la République Démocratique du Congo du 18 février 2006, préc) et en reconnaissant la personnalité juridique (Articles 211 et 212, loi n° 87/010 du 1er aout 1987 portant code de la famille telle que modifié par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er aout 1987, préc.).

¹⁷ Article 31, Constitution de la République Démocratique du Congo du 18 février 2006, préc.

¹⁸ T. MORGENROTH, *la vie privée en droit du travail*, thèse de Doctorat, Université du Droit et de la Santé Lille II, 2016, pp. 23 – 29.

¹⁹ J. MICHEL, « narrativité, narration, narratologie : du concept ricœurrien d'identité narrative aux sciences sociales », *Revue européenne des sciences sociales*, XLI-125, 2003, pp. 125-142

²⁰ Voir G. DELEUZE, *Cinéma 2* (1985), La théorie de la dividualité de Gilles Deleuze, développée notamment dans son « *Post-scriptum sur les sociétés de contrôle* » (1990) et anticipée dans ses travaux sur le cinéma, désigne la fragmentation de l'individu moderne en données divisibles. Contrairement à l'individu des sociétés disciplinaires (entier, enfermé), le dividual des sociétés de contrôle est un ensemble de traces, métadonnées, profils et codes. L'individu moderne n'est plus une entité close, mais un flux de données, un agrégat de comportements traçables (historiques de navigation, géolocalisation, achats) qui constituent son "profil". Antoinette Rouvroy prolonge cette analyse avec le concept de « *gouvernementalité algorithmique* ». Elle montre comment nos données, agrégées et analysées, nous gouvernent avant même que nous soyons conscients de nos propres choix. Les individus deviennent des "corps numériques" désirants et désirables, combinés par des algorithmes. Ce contrôle n'a pas besoin de lieux physiques (prisons, usines) ; il s'exerce en continu à travers les réseaux, les mots de passe et la modulation des données.

²¹ Il s'agit notamment des profils, interactions, métadonnées.

²² B. LOLEKA RAMAZANI « Le droit congolais face aux enjeux de protection de l'identité numérique : quel regard prospectif ? », in *Droit-Numérique.cd*, Dossier N° 5, Janvier 2025, p. 3.

Ces informations ont la caractéristique d'être conscientes, volontaires et plus ou moins contrôlées par leur producteur²³.

La seconde est l'identité numérique calculée. Elle regorge, quant à elle, les traces de navigation, plus ou moins conscientes et, dans tous les cas, involontaires. Le simple fait de naviguer sur Internet produit ces traces de connexion sur les différents sites visités²⁴. La troisième catégorie est l'identité numérique agissante. Cette dernière n'est pas produite par l'individu lui-même mais par d'autres internautes. Ces informations diffusées par des tiers à notre propos constituent, a priori, la forme la plus inédite de notre identité numérique.

Depuis 2000, l'accès à Internet progresse fortement en RD Congo. Au début, moins de 1 % de la population se connecte, surtout dans les cybercafés de Kinshasa et Lubumbashi. Entre 2011 et 2018, l'Internet mobile transforme la situation. C'est la période de l'accès haut débit (*ADSL*), remplaçant les connexions lentes et bruyantes. L'arrivée de la 3G/4G et la baisse des prix des smartphones démocratisent l'accès aux réseaux sociaux numériques.

Vers 2017, environ 20 % de la population utilise Internet. De 2019 à 2023, l'expansion s'accélère. Le taux de pénétration passe de 20 % à plus de 30 % en 2024. Les abonnés mobiles dépassent 28 millions et le trafic quadruple. En 2024-2025, entre 27 % et 50 % de la population est connectée. Les jeunes utilisent Internet surtout les réseaux sociaux numériques, le streaming et le commerce électronique. Cette croissance rapide alimente la construction de l'identité numérique, fragmentée mais omniprésente.

L'identité numérique du salarié en RD Congo se forme dans un espace transfrontière²⁵. Cet espace est dominé par des plateformes exerçant une forme de souveraineté technique. Elle échappe à l'emprise normative de l'État congolais. Les géants du numérique de la Silicon Valley imposent ses normes et usages. Dès lors, l'identité numérique du salarié se trouve façonnée par des logiques numériques et économiques largement extérieures au droit congolais.

Les salariés congolais participent eux-mêmes au processus d'auto-construction de l'identité numérique. Les outils numériques deviennent des supports de mise en forme de soi. Cette construction reste encadrée par les logiques des plateformes. Elle expose ainsi à un risque d'hétéronomie souvent sous-estimé²⁶.

Dans les sociétés contemporaines, la présence numérique est devenue un vecteur essentiel d'accès à l'information, à l'emploi et aux opportunités économiques. Les profils professionnels en ligne et les publications participent à la construction d'une e-réputation. Cette dernière est susceptible d'influencer favorablement la perception professionnelle d'un individu²⁷.

En effet, l'identité numérique s'exprime par les données personnelles. Ces dernières permettent d'identifier ou de profiler une personne de manière directe ou indirecte. La conception de la donnée personnelle, issue du modèle européen, s'inspire du régime général de protection des

²³ F. GEORGES, « représentation de soi et identité numérique : Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 », *op.cit.*, p. 3.

²⁴ *Ibidem*, p. 4.

²⁵ V. MILAD DOUEIHI, *Pour un humanisme numérique*, Paris, Éditions du Seuil, 2011, p. 177. La perspective de l'humanisme numérique développée par Milad Doueïhi nous permet d'appréhender les dynamiques contemporaines des données comme des faits culturels autant que techniques, ce qui éclaire particulièrement les enjeux congolais. Dans un contexte de circulation transnationale des données, l'identité numérique excède les cadres classiques du droit étatique pour devenir une construction éclatée, traversée par une pluralité de normes et d'acteurs. Elle s'inscrit ainsi dans une logique transjuridictionnelle, où les souverainetés nationales peinent à exercer un contrôle effectif sur des flux informationnels déterritorialisés.

²⁶ M. FOUCAULT, *Technologies of the Self*, in L. H. MARTIN, H. GUTMAN et P. H. HUTTON (dir.), *Technologies of the Self: A Seminar with Michel Foucault*, University of Massachusetts Press, 1988, p. 16-49.

²⁷ G. CLAUZET, *Identité numérique et économie de l'attention : des connaissances et des pratiques des jeunes lycéens*, Mémoire de Master, Université de Toulouse, 2015, p. 6.

données (RGPD)²⁸. Le RGPD définit la donnée personnelle comme toute information se rapportant à une personne physique identifiée ou identifiable²⁹.

Le Code du numérique définit aussi la donnée personnelle sans être en déphasage avec La loi n°20/017 du 25 novembre 2020 relative aux télécommunications³⁰. La donnée personnelle est tout élément permettant d'identifier directement ou indirectement une personne³¹. Il y établit une différence nette avec des données publiques qui traduisent l'action de l'État ou de ses institutions³².

À l'instar du RGPD, qui consacre une conception extensive de la donnée personnelle. Il impose un encadrement rigoureux du traitement des données des salariés. Ce qui reflète une culture européeniste de la donnée centrée sur l'individu. À l'inverse, le droit congolais reprend une définition et principes similaires au RGPD. Toutefois, cet appareil normatif semble non équivalent au contexte social et culturel de la conception congolaise de la donnée personnelle³³.

En pratique, cette différence se traduit par une protection moins structurée face aux dispositifs de surveillance numérique dans les relations de travail. Le RGPD rééquilibre le rapport de subordination par des garanties effectives. Le droit congolais laisse subsister une marge d'appréciation plus large au profit de l'employeur. Il en résulte une protection encore embryonnaire de l'identité numérique du salarié dans l'environnement professionnel.

La donnée personnelle a un cycle de vie. Elle naît par la collecte, se conserve par le stockage, s'analyse par le traitement, se mobilise par l'utilisation, se préserve par la sauvegarde, se réemploie par la réutilisation, et s'éteint par la suppression. À chacune de ces étapes, dans les relations du travail en RD Congo, des pratiques vont à l'encontre des principes de traitement des données personnelles des salariés³⁴.

En droit congolais, ce cycle se trouve juridiquement encadré. Le Code du numérique soumet à la régulation le traitement des données personnelles par tout acteur à des fins non domestiques³⁵. Ce dispositif vient compléter la loi n°20/017 du 25 novembre 2020 qui avait déjà esquissé le principe de confidentialité dans le traitement des données³⁶.

À l'inverse, l'identité numérique aussi comporte des risques significatifs pour les salariés congolais. La difficulté réside dans la persistance des données numériques. Contrairement aux interactions traditionnelles, les traces numériques sont durables, reproductibles et difficilement effaçables³⁷. Des informations erronées, décontextualisées ou obsolètes peuvent porter atteinte durablement à la réputation d'une personne.

²⁸ E. NETTER (sous Dir.), V. NDIOR, J.-F. PUYRAIMOND et S. VERGNOLLE, *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, Col. Colloque, Paris, 2019, p. 26.

²⁹ Article 4 point 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). *Aux fins du présent règlement, on entend par : 1) est «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); 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;*

³⁰ Article 4 point 37, loi n°20-017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication en RDC, préc.

³¹ Article 2 point 30, ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

³² Article 2 point 31, ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc. *La donnée publique est produite, gérée et stockée dans les registres publics de données sur le territoire de la République Démocratique du Congo dans le cadre d'une mission de service public par l'État, les provinces, les entités territoriales, les services, établissements et organismes publics ainsi que les personnes morales de droit privé chargées d'une mission de service public.*

³³ Droitnumérique.cd : « conception culturelle de la protection des données personnelles en RD Congo, webinaire à l'occasion de la journée internationale de la protection des données le 28 janvier 2026, disponible en ligne sur [https://www.youtube.com/watch?v=qW1RRB49pQk], consulté le 16 mars 2026.

³⁴ A. MONTEBRAN, *Cycle de vie des données, Notes de cours*, Master 2, Sénégal, 2024, p. 3.

³⁵ L'article 184, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, préc.

³⁶ Article 4 point 37, la loi n°20/017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication, préc.

³⁷ N. ANTONIN, « Les risques liés à l'identité numérique pour l'accès aux services publics L'exemple de FranceConnect », *Chronique de Andese*, 2023, p. 12.

À Kinshasa, près de 90 % des recruteurs effectuent des recherches en ligne avec les données du candidat. Une part importante, soit 70% a déjà écarté des candidats en raison du contenu de leurs activités sur les réseaux sociaux. Des traces anciennes publications sorties de leur contexte, influencent des décisions professionnelles. Le tri ne repose plus uniquement sur les qualifications. Il s'étend à la é-réputation³⁸.

Dans la classification des données personnelles énumérées par le code du numérique congolais, les données professionnelles occupent une place singulière. Elles englobent les informations relatives au statut, à l'emploi occupé, à l'employeur ou encore à la rémunération³⁹. Néanmoins, elles ne sont pas seules à être soumises au traitement par l'employeur⁴⁰.

Dans les entreprises privées, la e-réputation est un facteur de stigmatisation sociale et professionnelle. Les anciennes données toujours disponibles en ligne les salariés ne savent pas user de leurs droits à l'effacement et à la rectification à l'égard des responsables de traitement. Cette situation est particulièrement préoccupante dans les relations de travail en RD Congo. Les décisions de recrutement, d'évaluation ou de licenciement sont influencées par des éléments issus des activités numériques.

De nos jours, le candidat se présente rarement sous la seule forme d'un dossier papier⁴¹. Les plateformes de recrutement en ligne, les réseaux professionnels, les bases de données partagées et les outils d'analyse algorithmique transforment la sélection du personnel en un exercice de data-profiling⁴². L'employeur n'examine plus seulement un curriculum vitae imprimé mais encore et surtout il pénètre puis interprète une empreinte numérique des traces des activités en ligne du candidat. L'employeur devient alors un responsable de traitement des données du salarié pendant l'exécution du contrat de travail voire après l'exécution.

II. IMPACTS ET RETOMBÉES DE L'IDENTITÉ NUMÉRIQUE DANS LES RELATIONS EN R.D CONGO

Au fur et à mesure, l'univers du travail en RD Congo se digitalise. On vit l'époque de la plateformisation des relations de travail. Dans le cadre de ses prérogatives l'employeur, traite des données de ses salariés pour l'exécution du contrat de travail. En ce sens, notre analyse met d'abord en évidence les tensions entre les exigences de contrôle de l'employeur et le respect de la vie privée du salarié (II.1). Ensuite, il est impérieux d'examiner le cadre institutionnel de protection de son identité numérique ainsi que ses perspectives (II.2).

II.1. Tensions entre exigences de contrôle de l'employeur et respect de la vie privée du salarié

L'exécution du contrat de travail constitue une cause légitime de traitement des données personnelles des salariés. Néanmoins, cette base légitime ne saurait justifier une surveillance illimitée ou disproportionnée sur les salariés. La difficulté réside ainsi dans la recherche d'un équilibre entre les nécessités de contrôle de l'employeur et les limites de la sphère privée du salarié. Il convient d'examiner, les conditions d'une conciliation pratique entre vie privée et exécution du contrat de

³⁸ L'e-réputation, ou réputation numérique, désigne l'image en ligne (sur Internet) d'une personne, d'une entreprise ou d'une marque. Elle se construit à partir de l'ensemble des informations, avis, commentaires, photos et vidéos partagés sur les réseaux sociaux, les forums, les blogs et les moteurs de recherche.

³⁹ Article 183 point 3, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique en République Démocratique du Congo, préc.

⁴⁰ N. CHAMBARDON, *L'identité numérique de la personne humaine contribution à l'étude du droit fondamental à la protection des données à caractère personnel*, op. cit., p. 45.

⁴¹ Y.-M. LARHER, *les relations numériques de travail*, Thèse de doctorat en droit social, Université Paris II- Panthéon-Assas, École doctorale de droit social, 2017, p. 54.

⁴² *Ibidem*, p. 60.

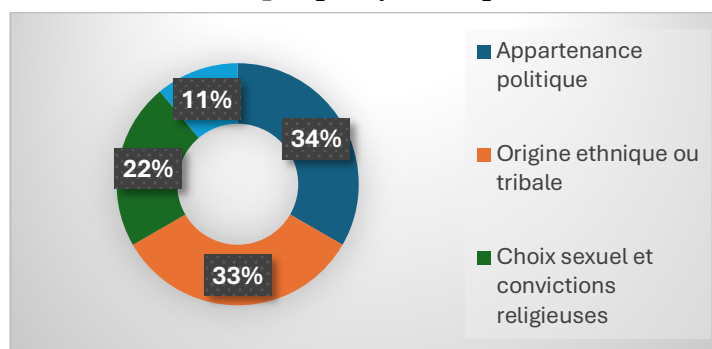
travail (1). Les technologies de surveillance (2) sont déployées en milieu professionnel comme instruments de contrôle.

1. Conciliation pratique entre vie privée du salarié et exécution du contrat de travail

En principe, le traitement des données personnelles exige le consentement libre et éclairé du salarié⁴³. Toutefois, dans les relations de travail, le consentement cède devant la base légitime que constitue l'exécution du contrat⁴⁴ réserve faite au traitement des données sensibles⁴⁵. Dans la pratique congolaise, l'exploitation des données personnelles révèle des discriminations significatives.

Notre enquête indique que 30 % des jeunes sont écartés en raison de leur appartenance politique. Par ailleurs, 30 % subissent une exclusion fondée sur leur origine ethnique ou tribale, traduisant la persistance du tribalisme. En outre, 20 % des cas concernent le choix sexuel ou les convictions religieuses, identifiés indirectement via les données en ligne. 10 % des exclusions reposent sur l'état de santé, l'employeur invoquant l'aptitude au travail pour justifier ces pratiques⁴⁶.

Graphique synthétique



Le principe de finalité interdit toute dérive dans l'usage des données⁴⁷. Les données des salariés sont légitimement traitées à des fins professionnelles. Or, la majorité des entreprises en RD Congo réutilisent ces données pour les publicités des produits et services de l'entreprise. Elles sont ensuite utilisées pour évaluer la performance. Ou pour surveiller les comportements. Et ce, sans information préalable du salarié. Cette réalité démontre la porosité des finalités, accentuée par l'absence de mécanismes internes de contrôle effectif.

À cette exigence s'ajoute celle de minimisation. Elle impose de limiter la collecte aux données strictement nécessaires⁴⁸. Pourtant, dans les pratiques observées en RD Congo, les sociétés touchent même à des informations qui n'ont rien à voir avec le travail⁴⁹. Les entreprises illustrent une tendance à la collecte extensive. Elles justifient cette tendance par des impératifs de sécurité mais qui vont à l'encontre des principes posés.

⁴³ Article 193 point 1, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

⁴⁴ E. DESTAILLATS, « Les nouvelles obligations de l'employeur en matière de protection des données personnelles des salariés », disponible en ligne sur [https://www.village-justice.com/articles/les-nouvelles-obligations-employeur-matiere-protection-des-donnees-personnelles,28756.html], (consulté le 10 janvier 2026).

⁴⁵ Article 2, point 32, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc. Les données sensibles regroupent des données biométriques, donnée à caractère personnel relative notamment aux origines raciales ou ethniques, aux opinions ou activités politiques, aux convictions religieuses ou philosophiques, aux appartenances syndicales, à la vie sexuelle, à la santé, à la génétique ;

⁴⁶ Article 38, loi n°015/2002 portant code du travail, préc. *L'embauche et le maintien en service sont subordonnés à la constatation de l'aptitude physique du travailleur via un certificat médical.* Article 1, arrêté départemental 28/75 du 30 octobre 1975 relatif aux examens d'embauche et de reprise, aux examens médicaux nécessités par l'exposition des travailleurs à des risques particuliers et à l'exercice des travaux légers et salubres.

⁴⁷ Article 193 point 1, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

⁴⁸ Article 243, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

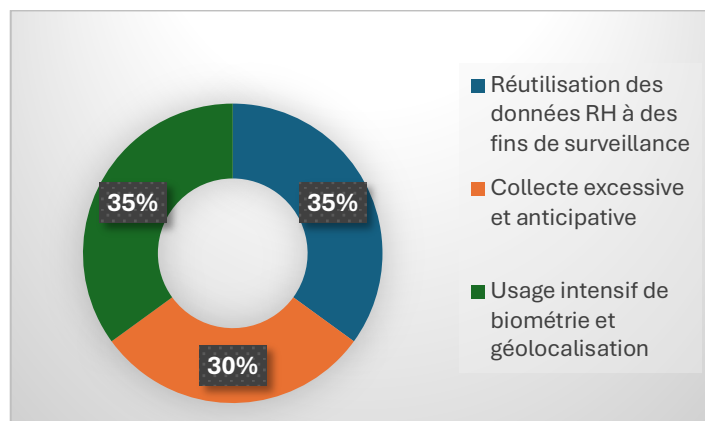
⁴⁹ Le fait par exemple de demander à un employé les informations sur ses origines ethniques et tribales, l'âge des parents et leurs métiers ou de savoir s'il a un parent ou allier dans la politique. La fiche de la Société Glencore RDC office de Curriculum demandent aux jeunes postulants des informations qui n'ont aucun trait avec le type d'emploi auquel il postule.

Le principe de confidentialité impose à l'employeur de garantir la sécurité des données⁵⁰. Il impose à l'employeur plusieurs obligations. L'employeur doit garantir la sécurité des données personnelles des salariés. Cette sécurité est à la fois technique et organisationnelle. La confidentialité limite l'accès aux seules personnes autorisées et encadre strictement leur utilisation. Toute divulgation devient une atteinte pouvant conduire à. En RDC, cette obligation se heurte à des contraintes techniques et organisationnelles. Dans certains cas, notamment dans le secteur bancaire, les données des salariés transitent par des plateformes numériques internationales. Ce qui occasionne les risques de fuite ou d'accès non autorisé.

Dans la pratique professionnelle congolaise, le traitement des données des salariés s'inscrit dans un écosystème élargi impliquant plusieurs acteurs. Les banques, les opérateurs de téléphonie mobile, les restaurants participent à la circulation des données des salariés. Cette pluralité d'intervenants complexifie l'identification des responsabilités et fragilise la protection de l'identité numérique.

Il ressort de notre étude empirique que 35 % des cas des violations des principes de protection des données dans les sociétés de télécommunications, les banques et les institutions de microcrédit. Les données RH sont réutilisées à des fins de contrôle de performance. Elle indique également que 30 % des cas relèvent des sociétés de restauration, des agences de voyage et de logistique. Ces situations traduisent une atteinte au principe de minimisation. La collecte des données est excessive et justifiée par des impératifs de prévention et de sécurité. 35 % des cas concernent les hôpitaux et les pharmacies. Ces pratiques démontrent une violation du principe de proportionnalité. L'usage des données sensibles est intensif et justifié par des contraintes médicales et organisationnelles.

Graphique synthétique



L'employeur est soumis à des obligations de loyauté et de respect de la dignité du travailleur⁵¹. Il est nécessaire de tenir compte des principes de traitement des données du salarié. Mais le bricolage technologique en Afrique met à l'épreuve cette exigence⁵². L'entreprise franchit la ligne de rationalité sur la sphère personnelle du salarié. Ces dispositifs visent la sécurité, mais ils engendrent une accumulation de données.

L'employeur n'est pas seul responsable de traitement. Le sous-traitant non contrôlé expose l'entreprise à des dérives⁵³. Les prestataires externes comme les cas fréquents en RD. Congo, les

⁵⁰ Article 131, loi n°20-017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication en RDC, préc.

⁵¹ Article 243, Ordonnance-loi n°23/010 du 13 mars 2023 portant Code du numérique, préc.

⁵² Y.-M. LARHER, *les relations numériques de travail*, op. cit.

⁵³ *Ibidem*

salariés sont payés via les banques commerciales. De plus, les sociétés fournisseurs des services numériques participent à la circulation et au stockage de ces données.

Le Code du numérique congolais dispense des formalités de déclaration préalable les traitements dont la publication est légalement prescrite⁵⁴. Dans l'ombre glacée de l'AUPSRVE⁵⁵, les données des salariés apparaissent comme de simples accessoires procéduraux. Elles sont livrées, sans égard à la dignité de la personne, réduites à de froids vecteurs d'exécution forcée. La logique d'efficacité créancière écrase toute prétention à une protection autonome des informations individuelles. L'employé devient ainsi un sujet passif d'investigations patrimoniales intrusives.

La donnée personnelle professionnelle⁵⁶ du salarié est exposée au nom de la rapidité procédurale de recouvrement des créances. Aucune architecture sérieuse de garantie n'est véritablement consacrée pour encadrer la circulation de ces données du salarié. Ce silence normatif révèle une carence structurelle préoccupante. L'exigence de recouvrement triomphe, au mépris d'un véritable droit fondamental à la protection des données des salariés.

Cette exception est conçue pour fluidifier la discussion dans les biens du débiteur. Elle incarne un instrument de contournement des garanties fondamentales du salarié. Et aussi, il faut rappeler le caractère social du salaire en droit du travail congolais⁵⁷. Cette situation légitime implicitement la circulation forcée d'informations sensibles entre juridictions, huissiers, banques et employeurs. Le salarié se trouve ainsi dépossédé de tout contrôle sur ses propres données, exposées au nom de l'efficacité de l'exécution.

L'exploitation des données à des fins de gestion stratégique se développe progressivement. Les entreprises utilisent les informations collectées pour produire des indicateurs de performance, orienter les décisions managériales ou structurer les carrières. Toutefois, l'absence de DPO traduit une sorte d'instrumentalisation de l'identité numérique. Ce qui conduit à des atteintes à la vie privée, voire à des usages détournés, comme l'illustre le risque émergent de manipulation des données ou de contenus numériques (notamment les deepfakes).

Les deepfakes sont des techniques d'intelligence artificielle capables de reproduire fidèlement un visage et de l'insérer dans une vidéo. L'image devient malléable et détachable de la personne réelle. À Kinshasa, ces procédés sont utilisés à des fins ludiques. Des visages souvent des dirigeants d'entreprises sont détournés et intégrés dans des scènes fictives et diffusées sans contrainte. Cette pratique traduit une banalisation de la réputation dans la manipulation numérique.

La référence aux deepfakes nous pousse à nous attarder sur les phénomènes d'usurpation d'identité numérique et de fraude au recrutement, dont la progression est désormais tangible. Ces questions gagneraient à être reprises et approfondies dans des analyses ultérieures.

⁵⁴ Article 189 point 2, Code du numérique RDC Préc.

⁵⁵ Acte uniforme OHADA relatif aux procédures simplifiées de recouvrement et des voies d'exécution, Journal Officiel OHADA, numéro spécial du 15 novembre 2023.

⁵⁶ Article 183, code du numérique RDC, préc. Les catégories suivantes sont considérées comme données personnelles. Il s'agit notamment de : point 3. Des données professionnelles : statut, emploi occupé, employeur, rémunération ;

⁵⁷ En droit du travail congolais, le salaire revêt un caractère social et alimentaire fondamental, protégé par la Loi n° 015/2002 portant Code du travail. Ce caractère est garanti par le principe de l'insaisissabilité partielle, la priorité en cas de faillite et le paiement obligatoire de salaire minimum. Articles clés du Code du travail de 2002 protégeant le salaire : 1) Article 91 : Institue la zone unique du salaire minimum interprofessionnel garanti (SMIG) et à ce jour, En RD Congo, la zone unique du SMIG est actée, avec une réforme confirmée portant le taux journalier du manœuvre ordinaire à 21 500 FC à partir de janvier 2026, après un réajustement à 14 500 FC début 2025. La Première Ministre maintient l'application de cette hausse, malgré les défis d'application du décret n° 25/22 du 30 mai 2025 portant fixation du salaire minimum interprofessionnel garanti, des allocations familiales minimales et de la contrevaletur du logement. Les articles 114-118 Règlent le mode de paiement (en monnaie légale), la périodicité et l'obligation de délivrer un bulletin de paie. Les articles 120-123 établissent les règles sur les retenues, la compensation de dettes et la saisissable, notamment l'insaisissabilité d'une partie du salaire pour assurer la survie du travailleur et de sa famille. L'article 124 accorde au salaire un privilège spécial, le plaçant en priorité absolue devant d'autres créanciers en cas de faillite ou de liquidation judiciaire de l'entreprise. Ces dispositions du Code du travail visent à garantir que le travailleur reçoive effectivement sa rémunération, protégeant ainsi le caractère alimentaire de ses revenus.

Le développement du télétravail en RD Congo révèle une surveillance accrue des salariés via les outils numériques⁵⁸. Ces derniers brouillent la frontière entre vie privée et vie professionnelle. Cette réalité s'illustre à l'instar le bricolage technologique africain. Des plateformes numériques comme WhatsApp sont détournées à des fins professionnelles informelles. Le télétravail congolais repose ainsi largement sur des canaux non encadrés par le hard law /soft law. En ce sens, la plateformisation du travail montre que l'identité numérique des salariés va se construire dans des plateformes étrangères. Cela traduit une inadéquation entre les pratiques numériques locales et le cadre juridique congolais encore insuffisamment adapté.

Le télétravail s'impose comme une pratique encore en structuration. Il est entrain de devenir essentiel dans la pratique congolaise depuis la période de Covid-19. À travers lui, le travail se dématérialise et le travailleur se manifeste par des identifiants⁵⁹. Chaque action professionnelle réalisée à distance laisse une trace numérique qui permet à l'employeur de mesurer la productivité du salarié⁶⁰. Pourtant, cette logique fonctionnelle s'accompagne d'un risque de surveillance constante. Le salarié congolais voit sa sphère privée se fondre dans son activité professionnelle, dans un espace virtuel où l'obligation de performance côtoie la menace d'intrusion⁶¹.

Le télétravail, souvent appréhendé de manière générique, gagnerait à être replacé dans les réalités infrastructurelles congolaises, marquées par des zones à faible connectivité. Ces contraintes techniques ne sont pas sans incidence sur la circulation sécurisée des données professionnelles. Une exploration plus fine de ces configurations pourrait utilement être poursuivie dans des travaux à venir.

La vérité sur l'identité numérique du salarié en RD Congo se situe à la croisée de deux logiques. L'entreprise cherche à maximiser son rendement, et celle de la dignité, que le droit doit préserver⁶². L'enjeu n'est pas seulement juridique, mais aussi éthique. La technologie amplifie le pouvoir de l'employeur et exige un équilibre par une responsabilité accrue. Le respect de la vie privée au travail devient un baromètre du degré de civilisation numérique d'une société⁶³.

2. Les technologies de surveillance dans les relations de travail

Pendant l'exécution du contrat, le traitement des données personnelles des employés est inévitable. L'entreprise, pour des raisons de sécurité, de productivité ou de gestion enregistre les données du salarié par des logiciels de suivi⁶⁴. Ce tissu d'informations compose un profil numérique interne du salarié. Il permet d'évaluer la constance, la rigueur, la présence, mais aussi, indirectement, la loyauté et la conformité à la culture organisationnelle⁶⁵.

Dans la pratique congolaise, les technologies de surveillance s'imposent progressivement comme des outils ordinaires de gestion du personnel⁶⁶. Les entreprises recourent à ces dispositifs

⁵⁸ J. PANZA, B. Kandolo, « L'histoire du numérique et ses défis réglementaires en République démocratique du Congo », in *Droit-Numérique.cd*, Dossier N° 1 – Juillet 2024.

⁵⁹ G. DEHARO, « au bureau ou à la maison ? Quand le télétravail bouleverse la relation de travail », in A la une, Actu grandes écoles, 2024, disponible en ligne [<https://www.mondedesgrandesecoles.fr/au-bureau-ou-a-la-maison-quand-le-teletravail-bouleverse-la-relation-de-travail/>], consulté le 17 octobre 2025. (Des connexions, des identifiants, des adresses IP, des signatures électroniques, ou encore des temps de connexion enregistrés).

⁶⁰ G. DEHARO, « au bureau ou à la maison ? Quand le télétravail bouleverse la relation de travail », *op. cit.*

⁶¹ N. LE BOUARD, « L'impact des technologies de surveillance sur les droits des salariés », in *village de Justice*, disponible en ligne, [<https://www.village-justice.com/articles/impact-des-technologies-surveillance-sur-les-droits-des-salaries,47028.html>], consulté le 17 octobre 2025.

⁶² Article 31, Constitution de la République Démocratique du Congo du 18 février 2006, préc.

⁶³ I. BA, *Le droit du travail à l'épreuve des nouvelles technologies de l'information et de la communication*, mémoire de Master en Droit de l'entreprise, Université Gaston Berger, 2002, p. 19.

⁶⁴ A. ALBERT, *santé au travail : l'heure de la digitalisation ? l'innovation technologique au défi de sa représentation de l'activité*, *op. cit.*, p. 66.

⁶⁵ Y.-M. LARHER, *les relations numériques de travail*, *op. cit.*

⁶⁶ Comme l'a pensé Shoshana Zuboff, dans *L'Âge du capitalisme de surveillance*, ce point cadre avec ses principales idées, en ce qu'il met en évidence une exploitation croissante des données personnelles à des fins de contrôle et d'anticipation des comportements. La pratique congolaise illustre, à son échelle, cette logique de captation et de réutilisation des données dans les relations de travail. Dans ce contexte, les technologies de surveillance s'imposent comme des outils de gestion interne. Les entreprises collectent et réutilisent les données des salariés au-delà des finalités initiales. Elles transforment les dispositifs techniques en instruments de contrôle continu. Cette évolution prolonge les constats relatifs à la porosité des finalités et à la collecte excessive des données.

dans un objectif affiché de contrôle de prévention des fraudes internes. Cette utilisation révèle des atteintes récurrentes aux principes de protection des données personnelles des salariés. Les sociétés privées utilisent des logiciels de suivi des performances⁶⁷. Ces outils enregistrent les connexions, les temps d'activité et les échanges professionnels. Les données initialement collectées pour la gestion administrative sont réutilisées à des fins d'évaluation individuelle. Le salarié ignore souvent l'étendue réelle du traitement.

Ces pratiques trouvent leur origine dans plusieurs réalités structurelles. Les entreprises évoluent dans un contexte marqué par la méfiance organisationnelle. Elles cherchent à limiter les pertes et à renforcer la discipline interne. Elles disposent de moyens technologiques croissants, mais sans encadrement juridique effectif. Les salariés, quant à eux, se trouvent dans une position de dépendance économique. Ils contestent rarement ces dispositifs.

Dans les supermarchés à Kinshasa⁶⁸, les caissiers travaillent sous vidéosurveillance constante. Certains dispositifs sont positionnés de manière rapprochée, parfois au-dessus des postes de travail. Ils permettent un contrôle permanent des gestes professionnels. Un comportement jugé suspect peut entraîner une sanction immédiate. Cette pratique traduit une présomption implicite de faute.

Dans les institutions financières, les systèmes de vidéosurveillance servent de fondement à des décisions disciplinaires⁶⁹. Dans les petites structures à Kinshasa, les pratiques sont encore plus informelles⁷⁰. Ces observations confirment que ces technologies sont utilisées comme des instruments de contrôle direct. Elles servent à surveiller, évaluer et sanctionner. Elles s'inscrivent dans un contexte marqué par l'absence de transparence et la méconnaissance des droits des salariés.

L'enquête révèle que la surveillance numérique se catégorise selon le type des secteurs⁷¹. L'employeur se réfugie souvent derrière l'argument de la sécurité informatique ou de la productivité. La protection de la vie privée⁷² impose désormais un cadre éthique à ces pratiques. Le contrôle doit être annoncé, justifié et limité dans le temps. Toute surveillance clandestine s'apparente à une faute et vicie la loyauté⁷³.

Pratiques de surveillance selon les secteurs en RD Congo

Secteurs d'activités	Technologies utilisées	Finalité affichée	Finalité réelle observée
Société de télécommunications et	Vidéosurveillance et Logiciels de suivi, monitoring IT	Gestion et performance	Surveillance individuelle et évaluation

⁶⁷ En RD Congo, plusieurs logiciels de suivi des performances sont utilisés dans les relations de travail. Voici les principaux outils identifiés : (Suite Tomate (Tom2 Pro) : Utilisée pour la gestion intégrée des entreprises, incluant la finance (tom2 Pro), les ressources humaines et la paie (tom2 Paie), la production d'états financiers (tom2 états Fin), le suivi-évaluation (tom2 Monitoring), la passation de marchés (tom2 Marché) et la gestion des stocks (tom2 Stock) ; DHIS2 (District Health Information Software 2), Implémenté à l'échelle nationale depuis 2013, c'est le principal Système d'Information de Gestion Sanitaire (SIGS) utilisé pour la planification et la gestion des programmes de santé au niveau national, provincial et dans les zones de santé ; Solutions RH : *SmartTeam est mentionné comme un outil de gestion des ressources humaines (RH) utilisé en Afrique.*

⁶⁸ Dans la pratique observée à Kinshasa, les supermarchés comme SK, Kin Marché, GG-Mart, Métro Mart, etc. recourent de manière systématique aux dispositifs de vidéosurveillance. Ces caméras sont installées aux caisses, dans les rayons et parfois au-dessus des postes de travail des salariés. Elles permettent un contrôle continu des activités, officiellement justifié par des impératifs de sécurité et de prévention des pertes. Toutefois, ces dispositifs servent également à surveiller le comportement des employés et à fonder des mesures disciplinaires. Dans la majorité des cas, les salariés ne sont pas informés de manière claire sur la finalité exacte de ces traitements, ce qui soulève des interrogations quant au respect des principes de transparence, de finalité et de proportionnalité en droit de la protection des données personnelles.

⁶⁹ Un contentieux devant la cour d'Appel du travail de Kinshasa Gombe illustre un cas au sein de Standard Bank Congo SA. Un employé est licencié pour vol sur la base d'images de surveillance. Il conteste les faits et saisit l'inspection du travail. Un procès-verbal de non-conciliation est établi. Il introduit ensuite une action devant le juge du travail. Le juge constate l'absence de preuve suffisante et le caractère abusif du licenciement. Il condamne l'employeur au paiement de plus de 70 000 dollars à titre de dommages et intérêts

⁷⁰ . Dans un restaurant à Kinshasa Pommes et Frites California, un salarié est licencié sans préavis ni décompte final. L'employeur fonde sa décision sur des images consultées à distance via son téléphone portable, connecté au système de vidéosurveillance. Le salarié n'est ni entendu ni informé préalablement. Cette situation illustre une confusion entre surveillance technique et pouvoir disciplinaire.

⁷¹ Z. BAUMAN, « Devoir de protection, protection des libertés : entre « surveillance liquide » et politiques sécuritaires », *op. cit.*, p. 48.

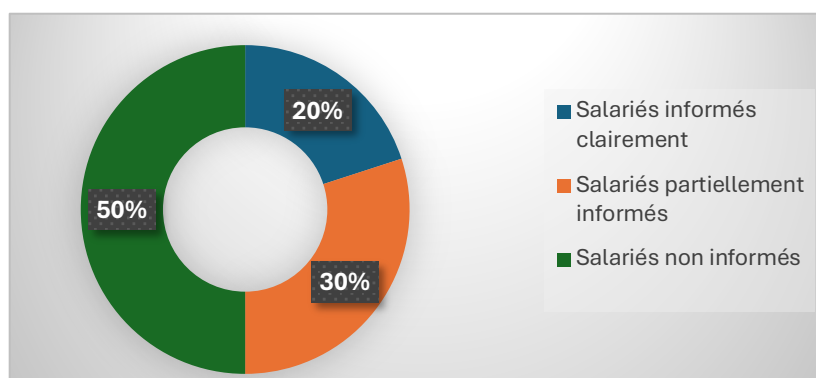
⁷² Article 31, Constitution de la République Démocratique du Congo du 18 février 2006, préc.

⁷³ T. PASQUIER, *L'économie du contrat de travail : conception et destin d'un type contractuel*, LGDJ, Paris, 2010, p. 97.

Banques commerciales			
Société minière, logistique et de transport des marchandises	Vidéosurveillance et Géolocalisation, biométrie	Sécurité et traçabilité	Contrôle permanent des déplacements
Société de Restauration et Super Marchés	Vidéosurveillance	Sécurité des biens de la société	Surveillance comportementale des salariés
Hôpitaux et Pharmacies	Vidéosurveillance, Systèmes numériques, traçabilité	Gestion médicale	Évaluation indirecte du personnel

Ce tableau met en évidence une dissociation entre les finalités affichées et les usages réels des technologies de surveillance. Les objectifs de gestion, de sécurité et de traçabilité servent de fondement à un contrôle individualisé des salariés. Dans plusieurs secteurs, les outils techniques sont détournés vers une surveillance continue des comportements et des performances. Cette pratique révèle une extension implicite des finalités initiales des traitements de données. Elle traduit une violation des principes de finalité et de proportionnalité en droit de la protection des données personnelles.

Présentation graphique de la perception des salariés sur la finalité des données collectées



Ce graphique met en évidence une asymétrie informationnelle significative dans la relation de travail en matière de traitement des données personnelles des salariés. Seuls 20 % des salariés déclarent être informés de la finalité des traitements, et encore de manière partielle. En revanche, 30 % des salariés présentent une connaissance incertaine. Ce qui traduit une compréhension fragmentaire des usages réels des données collectées. Enfin, 50 % des salariés indiquent ne disposer d'aucune information sur la finalité des traitements. Cette proportion majoritaire met en évidence une méconnaissance structurelle des droits des personnes concernées. Elle est révélatrice d'une violation manifeste des exigences de transparence et de loyauté dans le traitement des données personnelles des salariés.

Les conventions collectives sont prévues par le Code du travail congolais⁷⁴. Elles encadrent essentiellement les conditions classiques de travail. Dans la pratique congolaise, ces conventions n'existent pas en matière de protection des données personnelles des salariés. Cette absence révèle un retard face à la montée des pratiques de surveillance numérique. Dans plusieurs pays européens,

⁷⁴ Articles 272 à 296, loi n°015/2002 portant code du travail, préc.

les conventions collectives intègrent déjà des clauses spécifiques sur la protection des données des salariés, contrairement à la RDC⁷⁵.

Ainsi, la pratique congolaise révèle une généralisation des technologies de surveillance. Elle met en évidence un décalage entre les finalités déclarées et les usages réels. Elle souligne enfin une insuffisance de transparence à l'égard des salariés, en contradiction avec les exigences fondamentales du droit de la protection des données personnelles.

II. 2. Cadre institutionnel de protection de l'identité numérique du salarié et perspectives

Le droit congolais cherche à se structurer autour d'une cohérence interne capable de garantir la dignité numérique du salarié⁷⁶. Le chantier est vaste en ce qu'il ne s'agit plus seulement d'adopter des textes mais d'enraciner les principes dans le tissu institutionnel, professionnel et culturel du pays. Cette consolidation passe par une réaffirmation du rôle de l'État comme gardien de la donnée, mais aussi par une responsabilisation accrue des entreprises, appelées à devenir des acteurs de la confiance numérique.

1. Régulation comme pilier d'une protection de l'identité numérique des salariés

La régulation constitue le socle d'une protection préventive de l'identité numérique des salariés en droit congolais. Elle organise l'équilibre entre innovation technologique et sauvegarde des droits des salariés. L'ARPTIC, héritière de l'ARPTC, joue un rôle central en assurant la transparence et la sécurité des communications électroniques. Cependant, ces compétences de l'APD sont provisoirement transférées à l'ARPTIC⁷⁷.

L'Ordonnance-loi n° 23/010 du 13 mars 2023 a voulu rompre avec l'approche sectorielle sur la protection des données personnelles. Il érige la régulation en principe directeur. Ce principe structure un droit transversal. Il institue, d'une part, une autorité de régulation numérique⁷⁸. Il crée également une autorité de protection des données⁷⁹, d'autre part. Cette orientation politique manifeste une volonté de contrôler la gestion de la vie privée des salariés. La régulation devient donc la clef de voûte d'une gouvernance partagée entre l'État, les opérateurs économiques et les citoyens⁸⁰.

La régulation des données personnelles s'impose comme la matrice d'un nouvel ordre juridique dans l'environnement du travail⁸¹. En RD. Congo, elle ne se résume pas à un simple encadrement technique des communications électroniques. Elle constitue le fondement d'une éthique juridique où la technologie cesse d'être un instrument neutre pour devenir un enjeu de dignité et de responsabilité. Réguler, c'est civiliser le numérique⁸². C'est inscrire la donnée, le réseau, l'algorithme dans un ordre de valeurs que la loi détermine et que l'État garantit⁸³.

Néanmoins, la norme n'existe que si elle s'incarne dans des institutions. La régulation congolaise trouve aujourd'hui son centre de gravité dans l'ARPTIC. Cette dernière est venue remplacer

⁷⁵ En Allemagne, les accords d'entreprise (Betriebsvereinbarungen) encadrent l'usage des systèmes de surveillance et doivent respecter le RGPD avec des mesures de transparence et de limitation des données. En France et dans l'UE, le RGPD autorise expressément les conventions collectives à organiser la protection des données dans les relations de travail. Dans ces systèmes, les partenaires sociaux négocient directement les règles de surveillance numérique et de traitement des données. À l'inverse, en RDC, cette dimension reste absente des conventions collectives, ce qui laisse un vide normatif important dans la protection du salarié numérique.

⁷⁶ B. KANDOLO WA KANDOLO, « Régulation du numérique en rdc : L'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données », in *droit-numerique.cd, dossier n° 4, aout 2024*.

⁷⁷ *Ibidem*.

⁷⁸ Article 7, ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

⁷⁹ Article 162, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

⁸⁰ B. GOMES, *Le droit du travail à l'épreuve des plateformes numérique*, Thèse de Doctorat, Université Paris Nanterre, École doctorale 141 : Droit et science politique IRERP, 2018, p. 34.

⁸¹ *Ibidem*.

⁸² Article 3, Décret n° 23/13 du 3 mars 2023 portant création, organisation et fonctionnement de l'Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication du Congo, ARPTIC en sigle, préc.

⁸³ A. SUPLOT, « Pourquoi un droit du travail », *Dr. Soc*, 1990, p. 485

l'ARPTIC initialement créée par la loi n° 014/2002 du 16 octobre 2002⁸⁴. Le Décret de mars 2023 précise son organisation et son fonctionnement. Il confère à l'ARPTIC la personnalité juridique, l'autonomie financière et la mission de garantir le bon fonctionnement, la transparence et l'équilibre du marché des télécommunications, des TIC et de la poste⁸⁵.

Son rôle est d'ordinaire, celui d'un arbitre technique de veiller à la concurrence loyale, contrôler la qualité des services, attribuer les licences et réguler les interconnexions. Mais le décret de 2023 a bouleversé cet équilibre, en l'absence d'installation de l'APD prévue par le Code du numérique. Néanmoins, l'acte réglementaire confie provisoirement à l'ARPTIC les missions dévolues à l'APD⁸⁶. Cette situation exceptionnelle fait d'une instance sectorielle un organe de protection des libertés fondamentales, charge lourde et ambiguë.

L'extension des compétences de l'ARPTIC à la protection des données révèle une surcharge institutionnelle problématique. Elle cumule des missions techniques de régulation et des fonctions de garantie des libertés numériques. Cette hybridation affaiblit la spécialisation et la capacité d'action effective. Elle crée une confusion des rôles au détriment de la protection des salariés. Elle traduit ainsi une solution fragile et structurellement peu efficace.

L'APD devait incarner la garantie institutionnelle du droit à la protection des données. Elle devait être indépendante, dotée de pouvoirs d'enquête, de sanction et d'avis⁸⁷. Son absence, près de deux ans après la promulgation du Code, crée un vide pratique que le décret tente de combler par pragmatisme. Mais cette substitution met à nu la fragilité du dispositif congolais de régulation. Le modèle s'appuie sur une seule institution, déjà surchargée, pour exercer des compétences hétérogènes et parfois contradictoires⁸⁸.

L'ARPTIC se trouve ainsi à la croisée des chemins. Organe de régulation économique, elle devient gardienne de droits fondamentaux. Or, la logique de marché et la logique de liberté n'obéissent pas aux mêmes impératifs. Réguler la concurrence implique de stimuler l'innovation et la compétitivité, protéger les données personnelles suppose de limiter la circulation de l'information et de restreindre certaines pratiques commerciales. Entre efficacité économique et protection de l'identité numérique des salariés, le conflit est latent⁸⁹.

Dans la sphère professionnelle, cette tension se manifeste de manière aiguë. Les employeurs déploient des outils de gestion et de surveillance numérique qui collectent des quantités massives de données comme des horaires de connexion, géolocalisation, correspondances internes, empreintes biométriques⁹⁰. Ces informations, à la fois professionnelles et personnelles, constituent la trame de l'identité numérique du travailleur. L'ARPTIC, chargée d'en garantir la sécurité, se retrouve face à des enjeux qui dépassent son expertise technique initiale. Elle n'est pas conçue pour apprécier les atteintes à la vie privée sur le lieu de travail ni pour arbitrer les conflits entre employeur et salarié en matière de données⁹¹.

⁸⁴ Avis du Conseil d'État Congolais sous RITE 045 du 8 février 2022, Cfr. K. NDUKUMA ADJAYI, *Résumé écrits des séances de cours de Droit du Numérique*, L2 et M2 Droit, disponible en ligne sur [https://www.kodjondukuma.com/droit_num_pdf.php], (consulté le 08 novembre 2025). Le Conseil d'État Congolais, à travers un avis, a précisé que malgré l'adoption de la loi n°20/017 du 25 novembre 2020, l'ancienne loi n°014/2002 continue de produire effet tant qu'aucun acte réglementaire ne l'a formellement abrogée. Cette interprétation est fondée sur le principe de continuité du service public. Il a permis à l'ARPTIC de poursuivre légalement ses missions jusqu'à la création de l'ARPTIC par le Décret du 3 mars 2023.

⁸⁵ Articles 2 et 3, Décret n° 23/13 du 3 mars 2023 portant création, organisation et fonctionnement de l'Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication du Congo, ARPTIC en sigle, préc.

⁸⁶ B. KANDOLO WA KANDOLO, « régulation du numérique en RDC, l'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données », *op.cit.*, p. 2.

⁸⁷ J.F. HENROTTE, « Quelle est la procédure de sanction par l'APD ? », disponible en ligne sur [<https://lexing.be/que-faire-face-a-une-enquete-de-lautorite-de-protection-des-donnees/>], (consulté le 04 Octobre 2025).

⁸⁸ B. KANDOLO WA KANDOLO, « régulation du numérique en RDC, l'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données », *op.cit.*, p. 2.

⁸⁹ J.J. DUPEYROUX, M. BORGETTO, R. LAFORE, R. RUELLAN, *Droit de la sécurité sociale*, Dalloz, Paris, p.221.

⁹⁰ H. BOUCHET, « La surveillance numérique au travail », in *CNRS Éditions*, p. 101-117

⁹¹ B. KANDOLO WA KANDOLO, « régulation du numérique en RDC, l'ARPTIC investie autorité unique pour la régulation du numérique, la certification électronique et la protection des données », *op.cit.*, p. 2.

La régulation, en contexte professionnel, exige une approche humaniste du numérique. Elle suppose la mise en œuvre d'un droit à la transparence, d'un droit à la maîtrise et d'un droit à la désactivation numérique. L'employé doit savoir ce qui est collecté, pourquoi et jusqu'à quand⁹².

La protection des données en Afrique s'énonce avec solennité⁹³. Elle s'inspire de standards internationaux ambitieux. Elle prétend organiser un espace numérique de confiance pour les salariés. Elle proclame la garantie des droits fondamentaux face à la circulation des données. Elle consacre un encadrement ambitieux des traitements, y compris dans la sphère professionnelle⁹⁴. Mais, dans la pratique, elle se heurte à une circulation diffuse et banalisée des données des salariés. Elle révèle ainsi un écart persistant entre la norme proclamée et l'effectivité institutionnelle réelle.

Le Sénégal met précocement en place la Commission de Protection des Données Personnelles⁹⁵. Cette autorité s'inscrit dans une logique classique d'autorité administrative indépendante. Elle exerce un contrôle réel sur les traitements, y compris dans les relations de travail. Elle encadre progressivement les employeurs et impose des exigences de conformité. Cependant, la protection des données des salariés reste dépendante du niveau d'appropriation par les entreprises, ce qui limite son effectivité pratique⁹⁶.

Le Kenya institue une autorité centrale dotée de pouvoirs étendus de contrôle et de sanction. Cette autorité adopte une approche nettement plus coercitive à l'égard des responsables de traitement⁹⁷. Elle intervient concrètement dans les pratiques des entreprises. Elle contribue ainsi à discipliner les usages des données des salariés par des décisions visibles. Néanmoins, cette efficacité s'accompagne d'un risque d'hypertrophie du contrôle administratif sur les acteurs économiques.

Le Bénin met en place une autorité de protection dans une logique de consolidation progressive. Cette autorité affirme ses missions de contrôle et de sensibilisation sans encore imposer une contrainte forte⁹⁸. Elle tente d'encadrer les traitements liés à l'emploi dans un environnement encore peu structuré. Elle diffuse une culture juridique de la protection des données encore en phase

⁹² P.-A. CHARDEL, « Présentation générale. Nos existences sous surveillance. Regards croisés et perspectives critiques », in CNRS Éditions, pp. 9-27

⁹³ La protection des données en Afrique s'érige, depuis la Convention de Malabo en 2014, en exigence normative continentale. La Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles, également connue sous le nom de Convention de Malabo, a été adoptée le 27 juin 2014 à Malabo. Il se veut être un instrument de coopération continental ne pouvant entrer en vigueur qu'après la ratification par 15 États africains. La RD Congo est le dernier pays à ratifié la Convention de Malabo le 6 mars 2025 et les instruments de ratification ont été déposés le 27 juin 2025, au siège de l'Union Africaine.

⁹⁴ B. KANDOLO, « la ratification par la RDC de la Convention de Malabo : progrès juridique ou saut dans le passé ? », In *News-Juritech Droit-Numérique.Cd*, n°11, 28 juin 2025.

⁹⁵ La CDP est instituée par l'article 5, la loi n° 2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, et en application il y a le Décret n° 2008-721 en date du 30 juin 2008 portant application de la loi n° 2008-08 du 25 janvier 2008 sur la protection des données à caractère personnel. La CDP, composée de onze membres, a pour mission de veiller au respect de la légalité dans le traitement des données personnelles et de protéger la vie privée des citoyens sénégalais dans l'environnement numérique.

⁹⁶ C. NDEYE NGONE, « Sénégal : Situation effective de la protection des données personnelles », disponible en ligne sur [https://www.2bi.sn/senegal-situation-effective-de-la-protection-des-donnees-personnelles], consulté le 30 janvier 2026.

⁹⁷ Le Kenya a renforcé ses mécanismes de protection des données personnelles via la création d'autorités centrales à la data Protection Act, 2019 dans la loi sur la protection des données de 2019, No. 24 de 2019, la loi crée Office of the Data Protection Commissioner (ODPC) - Bureau du Commissaire à la protection des données. Il établit le Bureau du Commissaire à la protection des données (ODPC) en tant qu'autorité indépendante. Le Data Commissioner dispose de pouvoirs étendus pour procéder à des audits, des inspections et des perquisitions (sur mandat), mener des enquêtes et des procédures de plainte et imposer des sanctions administratives importantes (amendes pouvant aller jusqu'à 5 millions KES ou 1% du chiffre d'affaires annuel).

⁹⁸ La protection des données personnelles au Bénin est structurée par une démarche progressive, passant d'un cadre initial à une régulation numérique renforcée, incarnée par l'APDP (Autorité de Protection des Données Personnelles). Le cadre juridique a été initialement posé par la loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel. L'autorité actuelle, l'Autorité de Protection des Données Personnelles (APDP), a été établie et renforcée par la loi n° 2017-20 du 20 avril 2018 portant Code du numérique en République du Bénin. Cette loi consacre son Livre V à la protection des données personnelles. Le fonctionnement et la nomination des membres sont notamment encadrés par des décrets subséquents, tels que le décret n° 2021-092 du 10 mars 2021 portant nomination des membres de l'APDP. L'APDP adopte une approche pragmatique dans un environnement en structuration dans ses missions de Contrôle, conformément à l'article 483 du Code du numérique, l'APDP contrôle les fichiers, vérifie la conformité des traitements et peut mener des investigations, de sensibilisation où l'autorité met l'accent sur la formation et l'éducation des responsables de traitement, des employés et du public pour instaurer une culture de protection des données. Bien qu'habilitée à prononcer des sanctions, l'APDP privilégie dans un premier temps la mise en conformité et la sensibilisation, visant une montée en puissance progressive de la régulation.

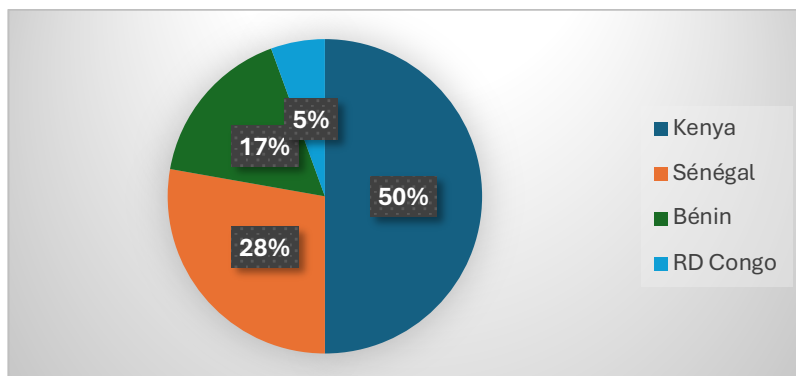
d'appropriation. Toutefois, la protection effective des données des salariés demeure limitée par la faiblesse des mécanismes de contrainte.

La réalité africaine démontre que les autorités existent, mais elles manquent souvent de moyens financiers, matériels et humains suffisants. Le contrôle demeure ponctuel et rarement systématique. La culture juridique de la donnée reste faible, tant chez les employeurs que chez les salariés. Les comportements sociaux favorisent la divulgation volontaire d'informations personnelles. Il en résulte un décalage manifeste entre la norme juridique et les pratiques sociales.

Fréquence générale de la protection des données en Afrique (échelle comparative du Sénégal, le Kenya, Bénin et de la RD Congo)

Pays	Existence réelle d'autorité de la protection	Activité réelle	Capacité de contrôle sur les entreprises	Fréquence globale de protection
Sénégal	Oui	Moyenne	Moyenne	Modérée
Kenya	Oui	Assez élevée	Assez élevée	Assez fréquente
Bénin	Oui	Moyenne	Faible	Rare
RDC	Non	Faible	Très faible	Inexistante

Présentation graphique de la fréquence de protection de l'identité numérique des salariés



Notre étude comparative révèle, avec une gravité certaine, une Afrique à géométrie variable en matière de protection des données. Le Kenya s'érige en modèle relatif, affichant une fréquence notable et une capacité de contrôle affirmée. Le Sénégal, quant à lui, incarne une régulation présente mais d'intensité mesurée, presque hésitante. Le Bénin illustre une fragilité structurelle, où l'existence institutionnelle peine à produire des effets concrets. Enfin, la RDC se distingue par une carence préoccupante, elle transfère les compétences de l'APD à l'ARPTIC. Ce qui traduit une quasi-absence de protection effective.

Il y a sur terrain la prééminence du Kenya, avec une fréquence culminant à 50 %, ce qui explique une effectivité entraînant d'avancer. Le Sénégal suit à 28 %, révélant une protection présente mais encore imparfaitement consolidée. Le Bénin, avec 17 %, témoigne d'une effectivité résiduelle, malgré un cadre institutionnel existant. La RDC, reléguée à 5 %, incarne une quasi-défaillance du dispositif de protection. L'ensemble esquisse une hiérarchie nette, où l'effectivité demeure profondément inégale sur le continent.

Ainsi, la régulation au service de la sphère professionnelle appelle une réforme structurelle. La mise en place effective de l'APD s'impose comme un impératif de sécurité juridique. Tant que cette institution reste confinée dans les textes, la protection de l'identité numérique des salariés demeure précaire, dépendante du bon vouloir administratif. La régulation, pour être effective, doit retrouver sa dualité entre un pôle économique incarné par l'ARPTIC, et un pôle libertaire incarné par l'APD. C'est à cette condition que le droit congolais pourra équilibrer l'efficacité technologique et la dignité humaine au travail.

Pour un conflit en matière de travail, quelle qu'en soit la cause, c'est le tribunal du travail qui en est compétent⁹⁹. Cette compétence s'exerce dans le respect des règles de procédure qui exige le respect de certains préalables procéduraux¹⁰⁰. Le juge congolais se trouve aujourd'hui à la croisée de deux exigences fondamentales, préserver l'autorité légitime de l'employeur et garantir, dans le même mouvement, la dignité numérique du salarié. Au fur et à mesure que l'entreprise s'informatise, la frontière entre la surveillance professionnelle et l'intrusion dans la sphère privée s'effrite¹⁰¹.

Le droit du travail contient des principes dont la portée s'étend naturellement à l'univers digital. Ainsi, le pouvoir disciplinaire, s'il reste un attribut essentiel du contrat de travail, ne peut se muer en une surveillance généralisée des données personnelles. Le juge, garant de cette proportion, est appelé à arbitrer entre la légitimité du contrôle et le respect de la vie privée numérique¹⁰².

Le contentieux du travail en matière numérique met ainsi en jeu la preuve électronique, dont la recevabilité dépend de la manière dont elle est obtenue. Le juge vérifie si l'employeur a respecté le principe de transparence et la finalité déclarée du traitement des données¹⁰³. À défaut, la preuve issue d'une surveillance dissimulée est écartée, car elle procède d'une atteinte illégitime aux droits du salarié. Dans une économie numérique où la trace électronique remplace le témoignage humain, cette exigence de loyauté probatoire devient une garantie fondamentale¹⁰⁴.

2. Nécessité de vulgarisation du métier D.P.O en RD. Congo et perspectives

La protection de l'identité numérique du salarié est une préoccupation majeure à l'ère où la donnée circule facilement. La désignation d'un délégué à la protection des données personnelles (D.P.O) s'impose comme une réponse normative essentielle. Cette fonction n'est pas spécifique à la RD Congo. Elle devient obligatoire pour les grandes entreprises s'inspirant de cadres juridiques internationaux¹⁰⁵.

Le DPO conseille et assiste le responsable du traitement dans toutes les questions relatives à la protection des données. Il informe et conseille les employés. Il surveille la conformité de l'organisation avec le droit applicable. Il assure la coopération avec les autorités de contrôle. Le cadre européen impose des garanties strictes d'indépendance sans recevoir aucune instruction quant à l'exercice de ses missions. Il fait directement rapport à la direction la plus élevée. Il ne peut être pénalisé ni licencié pour l'exercice de sa fonction si celui-ci est conforme aux obligations juridiques¹⁰⁶.

La législation congolaise adopte cette logique en ce que l'ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique impose à l'employeur de désigner un DPO. Ce dernier permet de

⁹⁹ Articles 15 et 16, loi n° 016 – 2002 du 16 octobre 2002 portant création, organisation et fonctionnement des tribunaux du travail.

¹⁰⁰ Articles 25 et 26, loi n° 016 – 2002 du 16 octobre 2002 portant création, organisation et fonctionnement des tribunaux du travail.

¹⁰¹ Z. BAUMAN, « Devoir de protection, protection des libertés : entre « surveillance liquide » et politiques sécuritaires », *op. cit.*, pp. 47 – 58.

¹⁰² C. LA HOVARY, *Les droits fondamentaux au travail : Origines, statut et impact en droit international*, Graduate Institute Publications, Genève, 2009, p. 16.

¹⁰³ Arrêt de la Cour de cassation Française du 18 juin 2025, Pourvoi n° 23-19.022. Il a été jugé que le droit d'accès n'est pas absolu : il peut être limité pour protéger les droits des tiers (secret des affaires, vie privée, données sensibles).

¹⁰⁴ P. LOKIEC, *Droit du travail, Tome I, Les relations individuelles de travail*, PUF, Paris, 2011, p. 117.

¹⁰⁵ M. DIAWA NSIMBA, « De la désignation du délégué à la protection des données en droit congolais », disponible en ligne sur [https://www.village-justice.com/articles/designation-delegue-protection-des-donnees-droit-congolais,47243.html], (consulté le 14 janvier 2026)

¹⁰⁶ F. BOISSART, « Le délégué à la protection des données, une fonction clé dans la gestion des risques », in *Village de Justice*, n°01, 2017, p. 3

garantir le traitement en bonne et due forme des données personnelles du salarié. Le D.P.O tient un registre des traitements et assiste le responsable du traitement dans toutes les phases du cycle de vie des données¹⁰⁷. Le code du numérique comporte une dispense de formalité pour les responsables de traitement qui désignent un D.P.O¹⁰⁸. Cette disposition démontre l'importance normative attachée à la fonction et consolide l'autonomie du D.P.O¹⁰⁹.

Selon l'ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, le Délégué à la Protection des Données est investi pour remplir les missions¹¹⁰ suivantes :

- Informer et conseiller le responsable de traitement ;
- Contrôler la conformité de collecte et traitement des données personnelles ;
- Conseiller sur les analyses d'impact ;
- Coopérer avec l'autorité de protection des données ;
- Être point focal pour l'autorité.

Tous ces éléments recommandent que le DPO ne détienne pas de fonctions impliquant la détermination des finalités et des moyens des traitements, afin de préserver son impartialité. Sur le plan doctrinal, cette exigence d'indépendance est fondamentale pour assurer un contrôle interne effectif. Elle évite que l'agent de conformité soit placé dans une position subordonnée aux logiques de gestion qui pourraient compromettre la protection des données.

En matière d'obligation légale, l'expérience européenne permet d'identifier des critères objectifs pour déterminer quand un DPO est requis. Le traitement à grande échelle de données sensibles, le suivi régulier et systématique de personnes, le traitement de catégories particulières de données. La législation congolaise s'inscrit dans cette dynamique¹¹¹.

Le droit congolais assouplit l'obligation pour les startups et les petites et moyennes entreprises (PME)¹¹². Celles-ci ne sont pas tenues de désigner un D.P.O sauf si leurs activités présentent un risque élevé pour les droits et libertés des personnes concernées. En pratique congolaise, les structures les plus nombreuses pourraient rester moins protégées. La figure du DPO demeure pensée pour des cadres formels. Elle interroge dans un contexte dominé par le secteur informel. Le risque est de réserver la protection des données à une minorité d'acteurs structurés. Cette piste mériterait, à elle seule, de faire l'objet d'analyses ultérieures plus approfondies.

La présence d'un DPO permet d'anticiper les risques juridiques et d'installer une culture de conformité. La protection de l'identité numérique du salarié exige une approche doctrinale exigeante et cohérente. La vulgarisation de la fonction de D.P.O s'impose. Elle implique la formation, la diffusion des bonnes pratiques et l'adoption de standards internationaux. Elle conduit à élever la protection des données à un niveau comparable aux systèmes les plus avancés, sans pour autant ignorer les spécificités économiques et sociales de la RD Congo.

En perspective, l'encadrement de l'identité numérique du salarié en droit congolais laisse entrevoir une volonté de structuration. Les textes existent et les intentions sont perceptibles. Mais leur mise en cohérence demeure incertaine. L'ensemble donne parfois le sentiment d'un édifice encore inachevé, où la norme peine à épouser les réalités effectives des relations de travail numériques.

¹⁰⁷ Article 222, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

¹⁰⁸ Article 189, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

¹⁰⁹ Article 225, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

¹¹⁰ Article 226, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

¹¹¹ Autorité de la Protection des données : « Dans quels cas est-il obligatoire de désigner un délégué à la protection des données », [<https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/delegue-a-la-protection-des-donnees/cas-obligatoires>], (consulté le 14 janvier 2026) ;

¹¹² Article 228 in fine, Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique, préc.

Dans ce contexte, une intervention du législateur apparaît souhaitable non dans une logique d'accumulation des textes mais dans un souci de clarification. Une première recommandation consisterait à renforcer l'harmonisation de la loi n°20-017 du 25 novembre 2020 et l'ordonnance-loi n° 23/010 du 13 mars 2023. Les deux textes abordent la même question sur la protection des données personnelles. L'unification des concepts et des régimes juridiques permettrait de réduire les incohérences actuelles. Elle offrirait également une meilleure sécurité juridique aux employeurs comme aux salariés.

En deuxième lieu, le premier ministre, détenteur du pouvoir réglementaire général, doit assurer une mise en ordre des dispositifs existants. Il peut préciser les conditions d'application des normes et fixer l'organisation et fonctionnement de l'APD. Les autorités sectorielles ne sauraient rester en marge. Le ministre en charge du numérique doit fixer des standards adaptés aux usages contemporains dans la relation professionnelle en collaboration avec le ministre du travail. L'absence de coordination entre ces deux pôles affaiblirait nécessairement la portée des règles en évolution.

En parallèle, le silence relatif des organisations syndicales interpelle. Leur rôle ne se limite pas à la défense classique des intérêts professionnels. Elles participent à la fabrication de la norme sociale. L'intégration de la protection des données des salariés dans les conventions collectives apparaît, à cet égard, comme une piste encore peu explorée. Une telle dynamique permettrait de rapprocher la règle des réalités du terrain, là où le droit étatique demeure parfois distant.

À l'égard des entreprises, les perspectives de conformité passent par l'intégration du délégué à la protection des données (DPO) comme acteur clé de la gouvernance interne. Le DPO ne doit plus être perçu comme un simple décideur technique. Il est un garant préventif des droits des salariés contre les abus. Il facilitera la détection des risques et conseillera stratégiquement la direction de l'entreprise. Cette évolution implique une professionnalisation du rôle, à travers des formations et une reconnaissance académique du métier. Ce qui commence à émerger grâce aux initiatives de formation dédiées en RD Congo.

Dans le même mouvement, la question de l'indépendance des Délégués à la protection des données mérite une attention particulière. Leur position au sein de l'entreprise demeure ambivalente. Elle oscille entre fonction de contrôle et dépendance organique. Dans cette perspective, l'émergence d'un réseau structuré de DPO, à l'initiative d'acteurs spécialisés tels que Droit numérique.cd, pourrait constituer un prolongement utile. À l'image des ordres propres aux professions indépendantes, une telle organisation contribuerait à consolider leur autonomie. Elle offrirait également un cadre d'échanges et de pratiques, susceptible de renforcer la crédibilité de leur intervention.

Ainsi envisagée, la protection de l'identité numérique du salarié ne relève pas d'un seul niveau d'intervention. Elle appelle une complémentarité des acteurs. À défaut, elle risque de demeurer cantonnée à un registre déclaratif, sans véritable prise sur les pratiques professionnelles. La mise en œuvre effective de ces normes doit s'accompagner d'une sensibilisation et d'une maturation juridique des acteurs, employeurs, salariés, autorités publiques et citoyens.

CONCLUSION █

La réflexion amorcée dans cette étude trouve son point d'aboutissement dans une prise de conscience profonde. L'identité numérique, dans les relations de travail, n'est plus une question périphérique du droit, mais un véritable enjeu de civilisation juridique. Dès l'introduction, le propos s'est attaché à décrire la genèse du problème. La dématérialisation progressive des rapports de travail bouleverse les repères traditionnels du droit du travail et interpelle la capacité du législateur congolais à garantir la dignité et la liberté du salarié à l'ère des données.

Le monde du travail en République démocratique du Congo connaît une digitalisation progressive et diffuse. Les données du salarié deviennent une ressource centrale de gestion. L'identité numérique s'impose comme un fait social observable et structurant. L'employeur mobilise les données personnelles pour organiser et contrôler le travail. Cette collecte s'appuie sur la base de l'exécution du contrat de travail. Mais l'usage déborde souvent le cadre strictement professionnel. Le contrôle numérique tend à s'étendre de manière continue et peu encadrée.

L'analyse empirique révèle des pratiques discriminatoires dans l'accès à l'emploi. Des exclusions apparaissent sur des critères politiques, ethniques ou religieux. Les données numériques servent indirectement à filtrer les candidats. Pendant l'exécution du travail, la surveillance numérique devient structurelle. Les entreprises utilisent des outils de suivi, de vidéosurveillance et de traçage. Les finalités déclarées de sécurité et de performance sont souvent dépassées. Le salarié évolue dans un environnement de contrôle permanent et invisible.

Les données personnelles circulent dans un écosystème professionnel élargi. Banques, télécommunications et prestataires participent à leur traitement. Cette pluralité d'acteurs rend la maîtrise des données difficile. La responsabilité devient diffuse et difficile à identifier empiriquement. Les résultats montrent aussi une faible transparence dans les traitements. Une majorité de salariés ne connaît pas la finalité des données collectées. Les principes de finalité, de minimisation et de proportionnalité sont fragilisés. L'usage réel des données s'éloigne des normes juridiques affichées.

L'observation du terrain met en évidence un déséquilibre structurel. Les pratiques numériques évoluent plus vite que les mécanismes de protection. Le salarié reste exposé à une surveillance continue et peu lisible. L'identité numérique devient ainsi un espace de tension permanente dans le travail.

BIBLIOGRAPHIE

I. CONSTITUTION

1) Constitution

- Constitution de la République démocratique du Congo, modifiée par la loi n° 11/002 du 20 janvier 2011 portant révision de certains articles de la Constitution de la République démocratique du Congo du 18 février 2006, JO RDC, 52^e année, n° spécial, 5 février 2011.

II. LÉGISLATION CONGOLAISE

1) Textes législatifs

- Loi n° 016 – 2002 du 16 octobre 2002 portant création, organisation et fonctionnement des tribunaux du travail.
- Loi n° 15/2002 du 16 octobre 2002 portant code du travail, telle que modifiée et complétée par la loi n° 16 du 15 juillet 2016, in J.O. RDC, numéro spécial du 15 juin 2016.
- Loi n° 87/010 du 1er aout 1987 portant code de la famille telle que modifiée par la loi n° 16/008 du 15 juillet 2016 modifiant et complétant la loi n°87-010 du 1er aout 1987, in J.O RDC, 15 juillet 2016.
- Loi n°20-017 du 25 novembre 2020 relative aux télécommunications et aux technologies de l'information et de la communication en RDC, in J.O. RDC, n° spécial du 22 septembre 2021.
- Loi organique n°13/011-B du 11 avril 2013 portant organisation, fonctionnement et compétences des juridictions de l'ordre judiciaire, JORDC, spécial, 4 mai 2013
- Ordonnance-loi n° 23/010 du 13 mars 2023 portant code du numérique en République Démocratique du Congo, in J.O RDC, numéro spécial du 11 avril 2023.

2) Textes réglementaires

- Arrêté ministériel de 2024, portant harmonisation des modalités de mise en œuvre des régimes du code du numérique et de la loi sur les télécoms et TIC.
- Décret n° 22/08 du 02 mars 2022 portant création d'une carte d'identité en République Démocratique du Congo.
- Décret n° 23/13 du 3 mars 2023 porte création, organisation et fonctionnement de l'Autorité de Régulation des Postes, des Télécommunications et des Technologies de l'Information et de la Communication du Congo, ARPTIC en sigle, Acte paru dans le n°Sp (première partie) du 7-03-2023 du Journal officiel.

III. LÉGISLATIONS INTERNATIONALE ET ÉTRANGÈRE

1) Législation internationale

- Déclaration universelle des Droits de l'Homme, adoptée à Paris, le 10 décembre 1948.
- 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
- Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel, adoptée à Malabo, 2014

IV. JURISPRUDENCE ÉTRANGÈRE

1) Jurisprudence Congolaise

- Avis du Conseil d'État Congolais sous RITE 045 du 8 février 2022 ;
-

2) Jurisprudence française

- Cour de cassation Française, Arrêt n° 23-19.022 du 18 juin 2025, (mails professionnels).

V. OUVRAGES

1) Ouvrages généraux

- BRUGUIERE (J.M.) et GLEIZE (B.), *Droit des personnes*, éd. Dalloz, Paris, 2023.
- CORNU (G.), *Vocabulaire juridique*, 10^{ème} éditions, PUF, Paris, 1987.
- GUINCHARD (S.), DEBARD (T.) et al, *lexique des termes juridiques*, éd. Dalloz, Paris, 2017.
- ILUNGA KASONGO (V.), *Code du travail modifié, complété et annoté*, éd. Nouveaux Elans, Kinshasa, 2019 ;
- KIFWABALA TEKIZAYA (J.P.), *Droit civil congolais : Les personnes, les incapacités et la famille*, éd. Presses universitaires de Lubumbashi, Lubumbashi, 2018.
- LEVY (J. P.) et CASTALDO (A.), *Histoire du droit civil*, 2^e éd. Dalloz, Paris, 2012.
- MATADI NENGA GAMANDA, *Droit judiciaire privé*, éd. Droit et Idées Nouvelles, Bruxelles, 2006.
- SAVATIER (R.), *traité pratique de droit civil français*, éd. LGDJ, Paris, 1952.

2) Ouvrages spécifiques

- BITAN (H.), *Droit et expertise du numérique, Créations immatérielles, Données personnelles, E.réputation, Droit à l'oubli, Neutralité, Responsabilité civile et pénale*, édition Lamy, collection Axe droit, 2015
- BOURGEOIS (M.), *Droit de la donnée, principes théoriques et approche pratique*, LexisNexis, Paris, 2017.
- BOUYA (E.R.) et K. NDUKUMA ADJAYI, *dématisation et gouvernance électronique*, éd. L'harmattan, Paris, 2020.
- DUPEYROUX (J.J.), BORGETTO (M.), LAFORE (R.), R. RUELLAN, *Droit de la sécurité sociale*, Dalloz, Paris.
- NDUKUMA ADJAYI (K.), *Cyberdroit, télécoms, internet, contrats de e-commerce, une contribution au droit congolais*, P.U.C., Kinshasa, 2009 ;
- NETTER (E.) (sous Dir.), V. NDIOR, J.-F. PUYRAIMOND et S. VERGNOLLE, *Regards sur le nouveau droit des données personnelles*, éd. CEPRISCA, Col. Colloque, Paris, 2019.
- PASQUIER (T.), *L'économie du contrat de travail : conception et destin d'un type contractuel*, LGDJ, Paris, 2010.
- SHOSHANA ZUBOFF, *l'Âge du capitalisme de surveillance*, éd. Zulma, Paris, 2020.
- SOUMAGNE (J.) (sous dir), *Mondes réels, mondes virtuels*, éditions du Comité des travaux historiques et scientifiques, Paris, 2021.

VI. ARTICLES

- ANTONIN (N.), « Les risques liés à l'identité numérique pour l'accès aux services publics L'exemple de FranceConnect », *Chronique de Andese*, 2023.
- BOISSART (F.), « Le délégué à la protection des données, une fonction clé dans la gestion des risques », in *Village de Justice*, n°01, 2017.
- BOUCHET (H.), « La surveillance numérique au travail », in *CNRS Éditions*.
- CHARDEL (P.-A.), « Présentation générale. Nos existences sous surveillance. Regards croisés et perspectives critiques », in *CNRS Éditions*.
- GEORGES (F.), « représentation de soi et identité numérique : Une approche sémiotique et quantitative de l'emprise culturelle du web 2.0 », in *Réseaux*, n° 154/2009.
- KANDOLO WA KANDOLO (B.), « Les transferts des données personnelles hors de la RD Congo », *Journal CODES Africa- Numéro 2- Vol 1*, Mars 2025, p. 2.
- LECLERC (O.), « Sur la validité des clauses de confidentialité en droit du travail », in *Droit Social*, 2005, n°2.
- MILLARD (E.), « Le rôle de l'état civil dans la construction de l'Etat », in *Centre de Théorie et Analyse du Droit*, n° 7074.
- NDUKUMA ADJAYI (K.), « Droit des données et service public de la donnée en République Démocratique du Congo », disponible en ligne sur [https://www.kodjondukuma.com/droit_donnees.php] publié en 2022 et révisé le 28 septembre 2023., (consulté le 17 octobre 2025).
- PERAYA (D.), « Les changements induits par les technologies », in *Actes du Colloque CETISIS-EEA 1999*, Montpellier, université de Montpellier II, Cépaduès, 4 et 5 novembre 1999.
- RIVOAL (I.), « Penser l'identité communautaire et les frontières sociales », *Dans Lucette Valensi à l'œuvre. Une histoire anthropologique de l'Islam méditerranéen*, Paris, Editions Bouquière.

VII. RESSOURCES EN LIGNES

- Autorité de la Protection des données : « Dans quels cas est-il obligatoire de désigner un délégué à la protection des données », [<https://www.autoriteprotectiondonnees.be/professionnel/rgpd-/delegue-a-la-protection-des-donnees/cas-obligatoires>], (consulté le 14 janvier 2026) ;
- BECCHIA (C.) et CHAMBODUC DE SAINT PULGENT (D.), « L'identité : introduction », in *Revue Pluridisciplinaire d'Etudes Médiévales*, p. 1-26, disponible sur [<https://journals.openedition.org/questes/2948>], (consulté le 06 octobre 2025).
- COUDOING (N.), *les distinctions dans le droit de la filiation*, thèse pour l'obtention du Doctorat en Droit Privé, Université du sud Toulon var, Faculté de Droit, le 23 novembre 2007.
- DEHARO (G.), « au bureau ou à la maison ? Quand le télétravail bouleverse la relation de travail », in *A la une, Actu grandes écoles*, 2024, disponible en ligne [<https://www.mondedesgrandesecoles.fr/au-bureau-ou-a-la-maison-quand-le-teletravail-bouleverse-la-relation-de-travail/>], (consulté le 17 octobre 2025).
- DESTAILLATS (E.), « Les nouvelles obligations de l'employeur en matière de protection des données personnelles des salariés », disponible en ligne sur [<https://www.village->

- justice.com/articles/les-nouvelles-obligations-employeur-matiere-protection-des-donnees-personnelles,28756.html], (consulté le 10 janvier 2026).
- DIAWA NSIMBA (M.), « De la désignation du délégué à la protection des données en droit congolais », disponible en ligne sur [https://www.village-justice.com/articles/designation-delegue-protection-des-donnees-droit-congolais,47243.html], (consulté le 14 janvier 2026)
 - HENROTTE (J.F.), « Quelle est la procédure de sanction par l'APD ? », disponible en ligne sur [https://lexing.be/que-faire-face-a-une-enquete-de-lautorite-de-protection-des-donnees/], (consulté le 04 Octobre 2025).
 - IRIGARAY (L.) « Le désir naît d'une différence plus que d'une similarité », in *philosophie Magazine*, propos recueillis par O. LARMAGNAC-MATHERON, le 29 avril 2021, disponible sur [https://www.philomag.com/articles/luce-irigaray-le-desir-nait-dune-difference-plus-que-dune-similarite], (consulté le 12 mars 2025).
 - LE BOUARD (N.), « L'impact des technologies de surveillance sur les droits des salariés », in *village de Justice*, disponible en ligne, [https://www.village-justice.com/articles/impact-des-technologies-surveillance-sur-les-droits-des-salaries,47028.html], (consulté le 17 octobre 2025).
 - NDUKUMA ADJAYI (K.), « Intelligence artificielle, désinformation algorithmique et cybersécurité ; protéger les journalistes et le public dans l'environnement numérique », in *conférence en commémoration de la 32ème journée mondiale de la liberté de la presse*, 05 Mai 2025, Fleuve Congo Hôtel, disponible en ligne [https://www.kodjondukuma.com/journee_presse.php], (consulté le 17 octobre 2025).
 - Rapport du Centre Henri Aigueperse, « L'impact de la transformation numérique sur les conditions de travail et d'emploi. Un aperçu général complété par deux études de cas Les chauffeurs-routiers dans le transport de marchandises et le personnel non-enseignant dans les établissements scolaires », in *Institut de Recherches Économiques et Sociales*, 2020
 - TASSEL (V.), « Infidélité d'un PDG américain : une relation amoureuse au travail peut-elle être un motif de licenciement en France ? », in *Le parisien*, disponible en ligne sur [https://www.leparisien.fr/economie/infidelite-dun-pdg-americain-une-relation-amoureuse-au-travail-peut-elle-etre-un-motif-de-licenciement-en-france-20-07-2025-SQ243HH5PNC7HJ756TGRRR4P6A.php] (consulté le 02 novembre 2025).

VIII. THÈSES ET MÉMOIRES

- CHAMBARDON (N.), *L'identité numérique de la personne humaine contribution à l'étude du droit fondamental à la protection des données à caractère personnel*, Thèse de Doctorat en Droit Public, Université de Lyon, 2018.
- MBALA MBALA (F.), *la notion philosophique de dignité à l'épreuve de sa consécration juridique*, Thèse de Doctorat en Sciences de l'Homme et Société, Université du Droit et de la Santé – Lille, 2007.
- CLAUZET (G.), *Identité numérique et économie de l'attention : des connaissances et des pratiques des jeunes lycéens*, Mémoire de Master, Université de Toulouse, 2015.
- ALBERT (A.), *santé au travail : l'heure de la digitalisation ? l'innovation technologique au défi de sa représentation de l'activité*, Thèse de Doctorat en sociologie, Université de Paris Est, 2023.
- BA (I.), *Le droit du travail à l'épreuve des nouvelles technologies de l'information et de la communication*, mémoire de Master en Droit de l'entreprise, Université Gaston Berger, 2002.

- GOMES (B.), *Le droit du travail à l'épreuve des plateformes numérique*, Thèse de Doctorat, Université Paris Nanterre, École doctorale 141 : Droit et science politique IRERP, 2018.

IX. NOTES DE COURS

- KALAY KISALA (P.), *Droit du travail -Notes de cours*, UPN, Faculté de Droit, 2023 – 2024.
- MUPILA DJIKE (H.F.), *cours de droit civil : les personnes*, Université Pédagogique Nationale, Faculté de Droit, première année de Graduat, 2019 – 2020.
- MONTEBRAN (A.), *Cycle de vie des données, Notes de cours*, Master 2, Sénégal, 2024.

Table des matières

I. DE L'IDENTITÉ CIVILE À L'IDENTITÉ NUMÉRIQUE	3
I.1. Identité en droit civil congolais	3
I.2. Extension vers l'identité numérique	4
II. IMPACTS ET RETOMBÉES DE L'IDENTITÉ NUMÉRIQUE DANS LES RELATIONS EN R.D CONGO.....	7
II.1. Tensions entre exigences de contrôle de l'employeur et respect de la vie privée du salarié	7
1. Conciliation pratique entre vie privée du salarié et exécution du contrat de travail	8
II. 2. Cadre institutionnel de protection de l'identité numérique du salarié et perspectives	14
1. Régulation comme pilier d'une protection de l'identité numérique des salariés	14
2. Nécessité de vulgarisation du métier D.P.O en RD. Congo et perspectives	18
CONCLUSION.....	21
BIBLIOGRAPHIE.....	22



Droit-Numerique.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 

