DE LA FALSIFICATION ELECTRONIQUE DES DOCUMENTS DANS LE SECTEUR EDUCATIF EN RDC : les enjeux des NTIC

YENDE RAPHAEL Grevisse
Professeur associé aux FAB

INTRODUCTION

L'usage des NTIC (*Nouvelles Technologies de l'Information et de la Communication*) se répand dans tous les aspects de la vie sociale et économique. Ces technologies évoluent à un rythme accéléré et leur transformation rapide rend aujourd'hui indispensable la parution d'une version sûrement nouvelle du plus ancien de ces œuvres. Leur rapide obsolescence requiert un ajustement constant des savoirs et savoir-faire. S'adapter n'est possible que si l'on dispose d'une solide connaissance des principes et des concepts de ce domaine étant donné qu'elle est une combinaison des technologies issues de l'informatique avec d'autres technologies apparentées, comme la communication, l'audiovisuel, les multimédias, l'Internet et les télécommunications qui permettent aux utilisateurs d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre l'information sous toutes les formes: texte, document, musique, son, image, vidéo, et interface graphique interactive[1].

Avec les Nouvelles technologies de l'information et de la communication, NTIC en sigle, la mondialisation entre dans une nouvelle phase historique : *celle de l'ère de l'information*. Les NTIC abolissent les distances, écrasent les durées, nous introduisent dans le monde de l'instantané et offrent une flexibilité longtemps recherchée. Elles présentent donc un substantiel avantage aux entreprises, et aux personnes qui sauront s'approprier ces nouveaux outils, face à une concurrence rendue plus âpre par la mondialisation. Les mots ne saurons l'exprimer, mais ces technologies ont impacté tous les secteurs de la recherche, de l'économie, du social, de l'éducation, etc. Les acteurs de l'économie sociale n'échappent pas à cette nouvelle donne et sont également confrontés à la nécessité de « *saisir* » les problématiques résultant de l'intégration de ces technologies au sein des systèmes institutionnels, recouvrant notamment les produits, les pratiques et les procédés afin de promouvoir leurs propres valeurs[2].

---

[1] *ARCEP, Étude sur le périmètre de la notion d'opérateur de communications électroniques,*
[2] *Krafft, J.: Profiting in the Info-Coms Industry in the Age of Broadband: Lessons and New Considerations. Technological Forecasting & Social Change, Vol. 77, p. 265-278*

Actuellement, les NTIC proposent de nombreux outils pour aider les chercheurs à créer des produits personnalisés. La plupart des ressources des recherches peuvent être numérisées avec l'assistance de l'ordinateur. L'utilisation de l'informatique dans la recherche a été promu dans de nombreux de pays dans le monde. Les chercheurs peuvent préparer leurs données et les faire à l'aide de l'ordinateur. C'est de nature à améliorer les méthodes traditionnelles. Cet impact des NTIC dans tous les secteurs de la vie sociale nous a beaucoup préoccupé et a conduit notre étude dans le secteur éducatif, plus particulièrement en République Démocratique du Congo, en illustrant d'une façon généralisée ses différentes facettes dans le secteur éducatif congolais.

Très peu d'études ont été consacrées aux problèmes de la falsification électronique des documents scolaires et académiques en RDC. Cependant, il sied de rappeler que l'informatique dans ses couleurs sur le plan éducatif produit des bonnes choses aussi bien qu'elle détruit. Et à la différence des générations précédentes où l'information constituait une denrée rare, les personnes du 21ème siècle, notamment dans les pays en voie de développement ainsi que les pays développés, vivent de plus en plus dans des environnements extrêmement riches en informations, et cette tendance va croissant. Cette surabondance informationnelle est notamment liée aux NTIC qui transforment l'information en un bien disponible, quasi-instantanément et indépendamment de la localisation géographique du producteur et du consommateur et à un coût relativement faible. Et bien que cette situation semble favoriser les conditions d'une concurrence pure et parfaite, il faut néanmoins tenir compte des capacités (*cognitives et attentionnelles*) récurrentes et limitées des individus[3], singulièrement face à l'efficacité des différents modèles du marché et des affaires qui, sont dorénavant remises en question par l'irruption des NTIC.

Sur ce, nous nous sommes proposés de mener une étude sur le sujet qui s'intitule « *De la falsification électronique des documents dans le secteur éducatif en République Démocratique du Congo : les enjeux des NTIC*», vue que l'avènement des nouvelles technologies durant ces dernières années au sein de la société a inféré le développement de nouvelles formes de délinquance dont les conséquences doivent être largement prises en compte, notamment par les opérateurs de communications électroniques et les différents utilisateurs dont chacun doit s'accorder à percevoir le risque y afférant comme le plus fréquent, et en revanche prendre de plus en plus conscience de la menace auquel nous sommes en permanence exposés.

---

[3] Progrès accomplis dans la mise en œuvre et le suivi des résultats du Sommet mondial sur la société de l'information aux niveaux régional et international, Conseil économique et social, Nations Unies, Genève, juillet 2013.

Par conséquent, cette étude se penchera sur l'impact des Nouvelles Technologies dans la falsification des documents scolaires et académiques en RDC, et par la même occasion, contribué à une compréhension plus ample des desseins des dernières dans la vie sociale.

Par ailleurs, Pour pallier à cette difficulté, plusieurs pistes de solutions pourront être envisagées, tant au niveau international qu'au niveau national, de la sorte qu'elles pourront aider des institutions universitaires a bien percevoir l'authenticité et la valeur des documents scolaires et académiques, par des moyens simples et actifs ainsi que dénicher les documents fraudés.

La démocratisation de l'éducation en République Démocratique du Congo exige d'être accompagnée par des réformes profondes ainsi la question qui fait l'objet de cette étude est : « *Existerait-il un modèle de référence organisationnel soutenant la lutte contre la falsification électronique des documents quant aux problèmes de l'authenticité et des résultats scolaires et académiques en RDC ?* ».

L'objectif capital de cette recherche est de démontrer les enchainements abusifs et les pratiques véreuse des NTIC dans le secteur éducatif en RDC, en conséquence, d'éviter la duplicité des documents scolaires et académiques indélicats en proposant de recourir à un établissement approprié et bien équipé quant à contrôler la circulation de ces documents dans tout le pays ainsi qu'à l'étranger.

Ce faisant, cette étude se propose pour objectifs spécifiques d' :

- Analyser et Appréhender le système d'octroi des documents scolaires et académiques en RDC,
- Interpréter et Proposer un prototype pratique de l'usage des NTIC quant à atteindre un niveau sécurisé des données concernant la circulation des documents scolaires et académiques en RDC,
- Instituer une politique nationale pouvant Permettre de constituer un système de circulation et de contrôle des documents scolaires et académiques dans tout le pays.

I. VUE D'ENSEMBLE DU SYSTÈME ÉDUCATIF CONGOLAIS : CROISSANCE ET EFFICACITÉ

Cette partie analyse en détail l'expansion de la scolarisation et la structure des flux des apprenants congolais; tout en prenant en considération les questions relatives à l'efficacité interne du système. Il identifie les problèmes prioritaires concernant l'accès et la progression des apprenants congolais; dans les différents niveaux d'enseignement. Les indicateurs examinés se rapportent seulement aux aspects quantitatifs du système, et ce, pour le pays dans son ensemble ; certaines inégalités sont néanmoins abordées : entre garçons et filles, entre provinces, entre riches et pauvres. Les questions concernant la qualité, en particulier au niveau primaire. Malgré les bouleversements politiques et de violents conflits, l'effondrement des recettes de l'Etat et la récession économique des 15 dernières années, le système éducatif de la RDC continue de se développer graduellement à tous les niveaux. Ce fait remarquable mérite d'être souligné alors que la plupart des services sociaux sont généralement jugés non fonctionnels.

L'expansion continue du système éducatif est d'autant plus impressionnante que les autres secteurs sociaux ont stagné ou régressé et que le déclin économique a été profond et durable. En outre, pendant plus d'une décennie, la RDC a reçu une aide au développement très faible ; le système éducatif a été soutenu entièrement par des efforts domestiques. Les chiffres officiels indiquent que le nombre d'établissements et les effectifs totaux se sont accrus dans le primaire, le secondaire et le supérieur. De façon surprenante, une enquête récente sur les ménages indique même que les taux de scolarisation dans le primaire pourraient être plus élevés que ne le suggèrent les données officielles ; bien que la qualité des données de cette enquête puisse être mise en doute, comme nous en discutons dans cette partie, elle confirme nettement une forte demande d'éducation et un engagement des parents à scolariser leurs enfants à l'école primaire.

Les effectifs universitaires ont doublé dans les années 2000 et le nombre d'apprenants congolais par rapport à la population est l'un des plus élevés d'Afrique francophone. Reconnaître ces succès, obtenus dans des circonstances extraordinairement difficiles, ne revient pas à nier ou à minimiser les défis considérables qu'il reste à relever, ou le retard que compte la RDC par rapport à d'autres pays[4].

[4] *la République démocratique du Congo au dernier rang de l'indice de développement humain du PNUD [archive], Le Monde, 15 mars 2013.*

Calculé sur la base des statistiques scolaires officielles et des projections de population, le taux de scolarisation de la population en âge de fréquenter l'école primaire reste faible environ 64 pour cent et semble avoir stagné depuis un certain temps, voire décliné depuis 15 ans ; le taux d'achèvement primaire est seulement de 24 pour cent ; le taux de survie dans le primaire est d'environ 44 pour cent ; et le taux d'efficacité interne est inférieur à 50 pour cent dans le primaire et le supérieur, ce qui traduit des taux élevés d'échec, de redoublement et d'abandon.

La Structure du Système primaire préconise une durée de l'enseignement obligatoire de 6 ans pour les enfants entre 6 et 11 ans. Bien qu'une scolarité préscolaire de 3 ans soit prévue, elle n'est offerte en pratique que dans quelques zones urbaines et pour une année ou deux, avec une classe pour les enfants de 5 ans et une classe unique pour ceux de 3 à 4 ans. La scolarité primaire de 6 ans est divisée en trois degrés de deux ans chacun. Le certificat de fin d'études primaires est accordé sur la base d'une évaluation des résultats en classe et des notes des apprenants à un test national (*autrefois le TENAFEP mais actuellement ENAFEP*).

L'enseignement secondaire, quant à lui, consiste en un cycle long et un cycle court. Pour le cycle long, Trois sections générales (*pédagogique, sociale et technique*) sont proposées. Ce cycle consiste en une première étape de deux ans dans un tronc commun aux trois sections, et une seconde étape de quatre ans qui introduit la différenciation entre les trois sections. Au sein de chaque section, diverses options sont offertes, jusqu'à trente options dans la section technique. Bien qu'il y ait une certaine spécialisation des établissements, comme dans certaines écoles techniques autonomes, et de nombreuses écoles secondaires, notamment à Kinshasa, offrent les trois sections et différentes options dans chacune d'elles.

Le cycle court, par contre, concerne l'enseignement professionnel qui consiste en une formation de 4 ans, qui commence immédiatement après l'enseignement primaire, ou une formation de 3 ans après le tronc commun du secondaire. Il y a trente-trois options dans l'enseignement professionnel[5]. En outre, il existe des écoles des arts et métiers qui offrent une formation à l'artisanat en trois ou quatre ans.

[5]*http://www.telesurtv.net/english/news/Development-Finance-Institutions-Funding-Land-Grabs-in-DR-Congo-20150602-0043.html*

L'entrée dans l'enseignement supérieur est conditionnée par l'obtention d'un Diplôme d'Etat qui sanctionne la fin du cycle long des études secondaires ; ce diplôme tient compte des résultats d'un examen national et du contrôle continu ; l'enseignement professionnel secondaire ne permet pas d'accéder à l'enseignement supérieur. Des concours d'entrée sont organisés par quelques rares établissements.

Quant à l'enseignement supérieur, il comporte un premier cycle de trois ans et un second cycle deux ans. Ces cycles d'études sont offerts dans des universités et des instituts non universitaires. Ceux-ci comprennent des instituts de technologie qui forment des techniciens (*les Instituts Supérieurs Techniques : IST*), des établissements pédagogiques qui forment les enseignants du secondaire, (*les Instituts Supérieurs Pédagogiques : ISP*) et des instituts qui combinent ces deux fonctions (*les Instituts Supérieurs Pédagogiques et Techniques, ISPT*). Les tableaux ci-dessous récapitulent succinctement toute la théorie sur l'organisation du système éducatif en RDC.

Tableau 1 : Structure du système éducatif en RDC

Niveau d'études	Type d'établissement	Âge théorique (années)	Niveau minimum d'entrée requis	Durée (années)	Certificat/diplôme délivré
Primaire				6	Certificat d'études primaires
Secondaire	Général	12–17	Certificat d'études primaires	6	Diplôme d'Etat d'études secondaires du cycle long
	Normal				
	Technique				
	Professionnel	12–16		5	Brevet/Certificat d'aptitude professionnelle
Université	Université	18–20/22		1er cycle-3 ans	Graduat
				2ème cycle-2 ans	Licence
				3ème cycle-2 ans	Diplôme d'Etudes supérieures
		Sans objet	Diplôme d'études supérieures	4-7 ans	Doctorat
Enseignement Supérieur	Institut Supérieur Pédagogique (ISP)	18–20/22	Diplôme d'Etat cycle long	1er cycle—3 ans	Graduat en pédagogie appliquée
				2ème cycle—2 ans	Licence en pédagogie appliquée

Source : Archive nationale de MINESURS

Tableau 2. Croissance du système éducatif en RDC– 1986/87 et 2001/02

		Etablissements		Enseignants		Etudiants	
		1986/87	2001/02	1986/87	2001/02	1986/87	2001/02
Préscolaire	Public non conventionné		16		138		1 530
	Public conventionné		74		388		7 745
	Privé		n.d.		n.d.		n.d.
Primaire	Public non conventionné	1 845	3 271	111 365	25 865	685 745	833 081
	Public conventionné	8 912	13 807		116 468	3 312 358	4 031 659
	Privé	378	2 241		16 498	157 929	606 237
Secondaire	Public non conventionné	4 107	1 761	41 696	23 747	292 196	353 452
	Public conventionné		5 269		70 870	606 081	1 045 861
	Privé	109	1 227		15 784	24 987	216 131
Supérieur	Public	36	114	8 557	7 897	45 731	170 000
	Privé		212		n.d.		30 000

Source : Archive nationale de MINESURS

Tableau 3. Croissance en pourcentage entre 1986/87 et 2001/02

		Etablissements	**Enseignants**	**Etudiants**
Primaire	Public Non conventionné	66%		21%
	Public conventionné	46%		22%
	Privé	480%		283%
	Total	65%	42%	31%
Secondaire	Public Non conventionné	65%		21%
	Public conventionné			72%
	Privé	1005%		764%
	Total	89%	164%	75%
Supérieur	Public	216%	–8,0%	271%
	Total	805%	n.d.	337%

Source : Archive nationale de MINESURS

II. DE LA REPRÉSENTATION DES FRAUDES INFORMATIQUES

L'avènement des nouvelles technologies durant ces dernières années au sein de la société internationale a induit le développement de nouvelles formes de délinquance dont les conséquences doivent être largement prises en compte, notamment par les opérateurs de communications électroniques. Si chacun s'accorde à percevoir le risque externe comme le plus fréquent, en revanche ils prennent de plus en plus conscience de la menace interne. Le rapport de l'observatoire national de la délinquance et des réponses pénales de 2011, recense, pour l'année 2011, 626 atteintes aux systèmes de traitement automatisé des données. Il s'agit principalement d'accès frauduleux dans un système (*par exemple: contournement ou violation d'un dispositif de sécurité, insertion d'un fichier espion enregistrant les codes d'accès des abonnés…)* ou de maintiens frauduleux dans un STAD[6] (*prolongation indue de l'accédant au-delà du temps autorisé, intervention dans le système afin de visualiser ou réaliser une ou plusieurs opérations…).* En outre, il faut préciser, toujours selon ce rapport, que plus du tiers de ces atteintes est constitué par des accès avec altération du fonctionnement, des modifications voire des suppressions de données. « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système automatisée de données : S.T.A.D* », est une infraction prévue par l'article 323-1, du Code Pénal informatique[7].

[6] *STAD : Système Automatisé de Données*

[7] *Elle vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la machine mais sur un système, qu'il procède à distance ou qu'il se branche sur une ligne de télécommunication. En outre, le mobile de l'accès frauduleux importe peu. On précisera qu'en l'absence de mise en place d'une protection ou de manifestation de volonté, par les dirigeants d'une entreprise, de restreindre l'accès au système informatisé de données, le délit de l'art. 323-1 du Code pénal n'est pas constitué. Ainsi, se rend coupable d'accès frauduleux dans un système de traitement automatisé de données voire d'introduction frauduleuse de données dans ce même système, la personne utilisant des codes d'accès confidentiels ne lui appartenant pas mais se faisant passer pour leur titulaire légitime, pousse une société à lui fournir un accès au réseau Internet. L'infraction susvisée a pour vocation de sanctionner les cyber délinquants qui cherchent à prendre connaissance d'informations, confidentielles ou non, figurant dans des système de données dont l'accès ou la présence leur est interdit. De ce fait, afin de qualifier l'infraction il conviendra d'une part de faire la preuve du caractère frauduleux de l'accès, et d'autre part, du caractère intentionnel de l'intrusion illicite. Il conviendra donc d'analyser tour à tour l'élément matériel puis l'élément moral du délit.*

II.1. L'ÉLÉMENT MATÉRIEL DU DÉLIT[8]

Le caractère protégé ou non du « *STAD* » n'est pas une condition requise à la qualification de l'infraction selon l'article 323-1 du Code Pénal, toutefois il facilitera la démonstration du caractère frauduleux de la « *pénétration* ». La preuve de l'accès frauduleux pourra, par exemple, résulter du contournement ou de la violation du système de sécurité mis en place par l'entreprise afin d'éviter ce genre d'attaques. En revanche, la preuve du caractère frauduleux de l'accès ne sera pas rapportée dans le cas où l'utilisateur est en situation normale, soit, s'il a procédé à une consultation d'informations rendues accessibles au public. Cette position a d'ailleurs été confirmée par la jurisprudence[9].

L'internaute ne peut donc être condamné sur ce fondement lorsque l'accès et le maintien dans le système de traitement automatisé était possible en accédant sur le site internet de la société à l'aide d'un simple logiciel de navigation grand public et ce, même si les données auxquelles il a ainsi pu avoir accès sont des données nominatives des clients de la société. Ainsi, les juges n'ont pas souhaité sanctionner l'accédant de bonne foi, qui d'après eux, n'avait pas accédé au « *S.T.A.D* » de manière frauduleuse[10]. De même, les juridictions considèrent que dans certains cas, l'accès n'est que le résultat d'une erreur: « *Le fait pour un centre serveur de s'approprier un code d'accès du kiosque télématique et d'y héberger un code clandestin n'est pas constitutif des délits d'accès, de maintien dans un système d'information de données informatisées et d'entrave* ». Cet accès a pu être le résultat d'une erreur de manipulation sur les fichiers. Par conséquent, l'action est dépourvue de caractère intentionnel[11] …

---

[8] « La cybercriminalité coûte plus cher que les trafics de cocaïne, héroïne et marijuana » , sur Le Monde.fr, consulté 8 Octobre 2016

[9] En effet, dans un arrêt du 30 octobre 2002, la Cour d'appel de Paris a considéré, qu'il « ne peut être reproché à un internaute d'accéder aux données ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès…». Il a ainsi infirmé le jugement de première instance, précisant les éléments constitutifs du délit d'accès et de maintien frauduleux dans un système de traitement automatisé de données.

[10] Jean-Loup Richet, « How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry into Cybercrime. », 17th AIM Symposium, 2012

[11] Toutefois, dans un arrêt rendu par la Cour d'appel de Paris le 9 septembre 2009, il a été jugé que l'accession ou le maintien frauduleux dans un S.T.A.D pouvait constituer un trouble manifestement illicite. A ceci près que, dans le cas d'espèce, l'accès aux données n'était pas limité par un dispositif de protection mais par le fait que le responsable du système avait manifesté son intention d'en restreindre l'accès aux seules personnes autorisées.

Il est nécessaire de démontrer le caractère intentionnel de l'intrusion illégale. Lorsque l'accès résulte d'une erreur, le simple fait de se maintenir dans le système pourra être constitutif d'une fraude[12]. En effet, une prolongation au-delà du temps autorisé, une intervention dans le système afin de visualiser une ou plusieurs informations constituent des indices permettant de participer à la démonstration du caractère intentionnel de la pénétration ou du maintien dans le système par l'utilisateur[13].

Outre, il faut rappeler que la loi incrimine non seulement le maintien irrégulier de l'accédant qui y serait entré par inadvertance, mais également celui de l'utilisateur qui y ayant régulièrement pénétré, s'y serait maintenu frauduleusement[14]. En application de l'article 323-1 du Code pénal informatique : « *la suppression, la modification, l'altération des données est punissable lorsqu'elles résultent d'un accès ou d'un maintien frauduleux dans le système* »[15].

II.2. DES ATTEINTES À L'INTÉGRITÉ DES SYSTÈMES D'INFORMATION[16]

Selon l'article 323-2 du Code pénal informatique est constitutif d'une infraction : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ». Ainsi la destruction de fichiers, de programmes, de sauvegardes, le flaming (*qui est une technique consistant à se livrer à des attaques via l'Internet en ayant la volonté de perturber le système d'information de son interlocuteur et de susciter un encombrement de sa capacité mémoire*), sont autant d'actes d'entraves constitutifs de cette infraction. On mentionnera plus particulièrement l'incrimination d'entrave d'un système de traitement automatisé de données par saturation…

---

[12] Le business de la cybercriminalité, Rodolphe Monnet et Franck Franchin, Hermès - Lavoisier, avril 2005

[13] Les infractions commises sur Internet, Abbas JABER, Thèse, Université de Bourgogne, France, novembre 2007

[14] Enfin, concernant la notion de maintien frauduleux dans un système, dans un arrêt du 5 avril 1994, la Cour d'appel de Paris a jugé que : « la loi incrimine également le maintien dans un système de la part de celui qui y serait entré par inadvertance, ou de la part de celui qui, y ayant régulièrement pénétré, se serait maintenu frauduleusement ». Par conséquent, peu importe la méthode utilisée pour pénétrer le serveur. Ce qui compte, c'est que le maintien existe et qu'il soit frauduleux, ce qui suppose la conscience pour les contrevenants de l'irrégularité de leurs actes. Cependant, pour que soit démontré ce maintien, il faut encore définir les contours de cette notion. Ainsi, le même Tribunal de Grande instance de Paris, dans un jugement du 15 décembre 1999 a défini la notion de maintien comme « l'action de faire durer ».

[15] Myriam Quéméner et Joël Ferry, Cybercriminalité : Défi mondial et réponses - 2ème édition, Perpignan, Economica, 9 mars 2009, 308 p.

[16] Le droit penal à l'épreuve de la cybercriminalité , Mohamed Chawki, Thèse, Université Lyon III, France, septembre 2006.

Il s'agira par exemple de l'entrave au fonctionnement du système par l'envoi massif de messages électroniques ayant pour conséquence de saturer la bande passante et les boites de réception de tous les salariés. Toutes formes d'activité étant en conséquence paralysées. A ce titre, nous citerons une affaire de février 2000 au cours de laquelle des sites Internet comme « *Yahoo!* »[17], « *eBay* », « *Amazon.com* », « *Buy.com* », ou encore « *CNN.com* », ont été pris d'assaut. Ces attaques qualifiées de « *déni de service* » ou « *denial of service* », se sont traduits par une saturation du site le rendant de ce fait inaccessible en submergeant de connexions le serveur qui l'hébergeait.

Par ailleurs, bien que les actes frauduleux commis par le prévenu l'ont été sur son lieu de travail et au moyen du micro-ordinateur fourni par son employeur, celui-ci doit être mis hors de cause dès lors que le salarié a agi à l'insu de son employeur, et que les actes qu'il a commis sont, sans contestation possible, étrangers au périmètre de la mission confiée[18]. Toutefois, en raison du caractère large des termes utilisés, dans un but de qualification de l'infraction d'entrave, certains agissements doivent être écartés, notamment, les entraves résultants d'une grève, celles engendrées par une suspension de fourniture de service ou enfin celles constituées par la rupture d'un contrat de fourniture de prestations de services informatiques.

---

[17]C'est par exemple, Concernant la célèbre affaire Yahoo, qui opposait plusieurs associations antiracistes, dont la Ligue Contre Le Racisme et l'Antisémitisme (Licra), aux sociétés Yahoo! Inc. et Yahoo France, s'est conclue en France le 20 novembre 2000 par une ordonnance de référé rendue par Monsieur Gomez Premier Vice-président du Tribunal de grande instance de Paris. Celle-ci ordonnait à l'entreprise américaine de : « prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis ». L'ordonnance a été rendue sur la base d'un rapport portant sur les possibilités techniques de filtrer l'accès au contenu litigieux pour le public français. En effet, le juge américain a considéré que la décision française était incompatible avec le premier amendement de la constitution des États -Unis qui garantit la liberté d'expression, ce dernier l'a donc déclarée inapplicable sur le territoire américain. Dans un autre registre, la jurisprudence a reconnu que devait être condamné pour altération au fonctionnement d'un système de traitement automatisé de données suite à un accès frauduleux, le salarié qui, depuis son nouveau travail et à l'aide du matériel mis à sa disposition, a intentionnellement saturé la bande passante de son ex-employeur en lui envoyant une grande quantité de courriers électroniques et de gros fichiers dans l'intention de lui causer un préjudice commercial.

[18] François-Bernard Huyghe, « Le cyberespace, nouvel enjeu stratégique [archive] », émission Géopolitique, le débat sur RFI, 23 septembre 2012

III. DE LA FALSIFICATION DES DOCUMENTS ELECTRONIQUES

Un faux document est un document dont le caractère authentique a été altéré : le document n'est donc plus conforme à la réalité. L'altération peut être:

- *Physique :* un document peut être modifié physiquement (*suppression d'éléments ou de références, ajout manuscrit d'informations altérant le document, par exemple*);
- *Intellectuelle* **:** le contenu du document n'est plus conforme à la réalité (*description inexacte des services rendus, contenu erroné d'un rapport, apposition de fausses signatures sur la liste de présence, par exemple*).

Tous les types de documents fournis par les bénéficiaires afin d'obtenir des subventions, de participer aux procédures d'attribution de marchés publics ou de solliciter le remboursement de dépenses sont susceptibles d'être falsifiés : *contrats; pièces d'identité; curriculum vitae; garanties bancaires; bilans; factures (sous format papier ou électronique); rapports; décompte horaires; listes de présence; sites internet et Autres.*

III.1. DE LA VALIDITE DES ORIGINAUX ET DES COPIES CERTIFIEES.

Quatre formes de documents entrent en ligne de compte : *le document original; une copie du document certifiée conforme; une copie simple du document et une version électronique du document.*

Les pratiques nationales régissant les conditions de présentation d'originaux ou de copies peuvent varier selon les pays. Dans tous les cas cependant, les bénéficiaires sont tenus de pouvoir présenter les originaux à la demande des autorités, sans préjudice des dispositions légales nationales et internes, les responsables géographiques doivent adopter une approche pragmatique garantissant un équilibre entre les contrôles de premier niveau indispensables et l'obligation pour les bénéficiaires de conserver leurs documents à des fins comptables, pour les besoins d'un audit, par exemple.

En cas de suspicion, les autorités de gestion sont tenues de mettre en place des mesures spécifiques en vue de la vérification des documents. Il convient de mettre l'accent sur l'efficacité des contrôles sur place. Par exemple, en cas de falsification présumée de la part d'un bénéficiaire souhaitant mener une opération spécifique, les autorités de gestion doivent permettre la réalisation des contrôles documentaires nécessaires et obtenir une vue globale de la capacité réelle de la société à mettre en œuvre le projet.

III.2. EXHORTATIONS D'ALERTE SUR LA BONNE GESTION DES DOCUMENTS EN RDC

Une exhortation d'alerte est un indicateur de fraude ou de corruption présumée. Il est constitué d'un élément ou d'un ensemble d'éléments s'écartant de la normalité ou qui, par leur nature, présentent un caractère inhabituel. C'est le signal d'une anomalie pour laquelle des recherches plus approfondies pourraient s'avérer nécessaires. La présence d'exhortations d'alerte doit renforcer la vigilance du personnel et des responsables et encourager ces derniers à prendre les mesures indispensables afin de confirmer ou d'infirmer la présence d'un risque de fraude. La réactivité est d'une importance cruciale. C'est aux autorités de gestion qu'il appartient de lever les doutes que le signal d'alerte a suscités. Il y a lieu de souligner que la présence d'exhortations d'alerte ne signifie pas pour autant qu'une fraude a été commise ou pourrait être commise. Elle indique seulement que la situation doit être vérifiée et contrôlée avec toute la diligence nécessaire.

III.2.1. SUR LE FORMAT DES DOCUMENTS

Par conséquent, il convient de s'interroger sur les documents dont la présentation s'écarte des normes établies et généralement admises notamment :

- des factures ou des lettres n'affichant pas le logo de l'entreprise;
- des factures imprimées sur un support papier autre que des formulaires préétablis;
- des différences visibles dans le type, la taille, la netteté, la couleur, etc., de la police de caractères utilisée dans le document;

- des chiffres effacés ou biffés, des suppressions non validées par la signature des personnes autorisées;
- des montants manuscrits ne portant pas la signature des personnes autorisées ou la présence d'éléments sur un document imprimé a priori non justifiés;
- absence ou présence inutile de lettres, discontinuité dans les lignes de texte;
- des cachets officiels présentant des bordures anormalement nettes ou des couleurs inhabituelles indiquant l'utilisation d'une imprimante;
- l'apposition de signatures de personnes parfaitement identiques (*format et taille*) sur plusieurs documents, évoquant la possibilité d'une falsification par impression informatique;
- et plusieurs signatures manuscrites réalisées dans un style comparable ou à l'aide d'un stylo identique sur des documents concernant des périodes différentes.

III.2.2. SUR LE CONTENU DES DOCUMENTS

- caractère insolite des dates, montants, annotations, numéros de téléphone ou calculs;
- inscriptions manquantes (*dans les vérifications séquentielles*);
- erreur de calcul dans une facture ou feuille de paie informatisée: par exemple, incohérence entre les montants totaux et la somme des opérations;
- absence d'une mention obligatoire sur une facture: date, numéro d'identification fiscale, numéro de facture, etc.;
- position respective identique du cachet et de la signature d'une personne dans un ensemble de documents, évoquant l'utilisation d'une image (*et non une signature authentique*) : il peut s'agir d'une image générée par ordinateur et utilisée à des fins de falsification;
- absence d'informations de contact concernant une entreprise ou une personne, comme le numéro de téléphone, par exemple;
- absence de numéros de série sur les factures ou les bordereaux d'expédition de marchandises généralement identifiées par des numéros de série (*produits électroniques ou issus de lignes de production, etc*.);
- description vague des biens et services;
- divergences et écarts par rapport à la norme dans les numéros de compte bancaire (*par exemple, nombre insuffisant de chiffres, numéro ne correspondant pas à une agence bancaire spécifique, autres incohérences visibles*).

III.3. METHODES DE DETECTION DE FALSIFICATION NUMERIQUE

La meilleure méthode de détection consiste à confronter un faux à la réalité. C'est en effet le moyen le plus rapide et le plus aisé d'obtenir les meilleurs résultats dans un processus tel que la détection, dans lequel le facteur temps joue un rôle crucial. Il y a lieu de mener des contrôles appropriés afin de répondre à des questions telles que :

- les institutions engagées dans une telle opération existent-t-elles réellement?
- l'institution publique concernée a-t-elle réellement émis ce document?
- qui sont réellement les personnes censées avoir pris part à une activité donnée?
- qui est le véritable propriétaire d'un actif donné?

III.3.1. ANALYSE FONDEE SUR LE RISQUE

Sur la base de l'expérience acquise au fil du temps, et dans le cadre spécifique de leurs activités et de leur zone de compétence géographique, il se peut que les autorités de gestion aient décelé des secteurs particulièrement exposés. Elles doivent attirer l'attention de leur personnel à l'égard de ces secteurs et instaurer des mesures et des contrôles spécifiques. Le risque de falsification ou d'altération de documents concerne divers types de documents et à différentes phases de la mise en œuvre d'un projet. Citons par exemple:

- la certification du respect des critères définis pour le cofinancement;
- le titre de propriété légal;
- la certification de l'exécution de travaux ou de la prestation de services, ainsi que l'acceptation de ces derniers;
- les factures et les documents de référence confirmant l'exécution de paiements;

III.3.2. RECOUPEMENTS A L'AIDE DE BASES DE DONNEES

Le recoupement des informations disponibles constitue pour les autorités de gestion un contrôle important de premier niveau, qu'elles peuvent effectuer notamment sur la base d'un échantillon. Le contrôle peut porter, entre autres, sur les informations relatives à l'enregistrement des sociétés et sur les données financières ou opérationnelles.

Un accès direct à l'internet permet au responsable géographique de s'assurer de l'existence d'une entité en confirmant l'adresse et les numéros de téléphone de cette dernière. Il fournit également un accès au site éventuel de l'entité, lequel offre d'utiles informations sur les moyens opérationnels et l'environnement de l'entité. Sans préjudice des législations nationales. C'est alors que les autorités de gestion peuvent demander l'accès aux bases de données ou aux informations de toute institution détenant des données utiles de manière indépendante et séparée (*par exemple, les institutions financières publiques responsables des questions fiscales*[19] *et de la délivrance de documents en la matière; les autorités publiques chargées de la propriété ou de l'identification foncière; le bureau de commerce compétent pour tout renseignement lié à la structure et à l'historique des sociétés; des autorités spécifiques délivrant des autorisations pour certaines activités, etc*.). Cependant, Les recoupements dans le cas d'opérations transfrontières peuvent se révéler plus difficiles à réaliser, toutefois, des recherches génériques sur l'internet peuvent également aboutir à des conclusions utiles.

III.3.3. CONTROLES SUR PLACE

Les contrôles sur place constituent un important outil pour la détection de faux documents. Ils permettent de s'assurer:

- de l'existence du bénéficiaire et, dans une certaine mesure, de la cohérence entre les éléments figurant dans les documents fournis dans le cadre de la soumission et la réalité ;
- que les copies de documents présentées lors de la demande de cofinancement / paiement (*que ce soit sur format papier ou électronique*) sont parfaitement conformes aux documents originaux se trouvant en possession du bénéficiaire;

[19] *Administration fiscale publique, organismes chargés du prélèvement des cotisations sociales, administration douanière, etc.*

- que les informations contenues dans le procès-verbal de réception et les factures correspondent bien à la réalité; en d'autres termes, que les travaux et services ont été effectivement réalisés conformément à ce qui a été déclaré.

III.4. LA FALSIFICATION EN CONTEXTE NUMERIQUE DANS LES INSTITUTIONS D'ENSEIGNEMENT EN RDC

Les institutions d'enseignement sont actuellement confrontées à une réalité indéniable : le développement du Web et de ses ressources ont radicalement modifié la recherche documentaire et la réalisation des travaux académiques. Étudiants, professeurs et professionnels œuvrant au sein des institutions de formation, tous recourent à Internet, qui met à la disposition de ses utilisateurs un ensemble de données et d'informations d'une ampleur phénoménale.

La génération, qui fréquente actuellement nos universités, est née et a grandi à l'ère numérique. Elle fait un usage généralisé du Web, s'en servant non seulement pour s'informer, mais aussi pour communiquer, créer et collaborer[20]. Une grande proportion des 18 à 30 ans est considérée comme de grands utilisateurs d'Internet : 40 % d'entre eux passent ainsi 21 heures ou plus sur le Web par semaine. Il va sans dire que la recherche documentaire en contexte universitaire et que la réalisation des travaux sont influencées par l'omniprésence des technologies dans la vie des étudiants. Toujours selon l'enquête menée par le CEFRIO, 91 % des étudiants de 16 à 30 ans utilisent un ordinateur pour réaliser leurs travaux; 29 % des universitaires sondés en emploient systématiquement un en classe.

Par ailleurs, une étude menée en 2006 en France par les sociétés Le Sphinx Développement et Six Degrés auprès de 975 étudiants provenant de divers établissements universitaires et de domaines variés[21] *(informatique, physique, biologie, sciences humaines, etc*.) a montré que 97 % des étudiants emploient Internet comme source principale de documentation. Questionnés sur les avantages obtenus à se servir d'Internet comme ressource documentaire, les étudiants ont donné, en ordre d'importance : *la rapidité d'accès aux informations (88 %), la variété des sources trouvées (77 %), la facilité de réutilisation des sources (36 %), et la qualité des sources trouvées (15 %).*

---

[20] La génération C rassemble les jeunes de 12 à 24 ans et a été nommée ainsi par le Centre francophone d'informatisation des organisations (CEFRIO) (Source : http://www.cefrio.qc.ca/index.php?id=31).

[21] http://www.compilatio.net/files/sixdegres-sphinx_enquete-plagiat_fev06.pdf

Ces résultats montrent clairement que le recours au Web dans la réalisation des travaux académiques occupe une place considérable dans les habitudes des étudiants d'aujourd'hui. Si Internet peut être considéré comme une ressource utile à l'apprentissage, l'importante démocratisation de l'information qu'il a entraînée comporte des inconvénients. Notamment, il semble légitime d'affirmer que l'accessibilité des informations fournie par Internet combinée à la facilité d'utiliser la fonction copier-coller aurait amplifié le phénomène du plagiat.

En effet, les étudiants pouvant accéder aisément aux données du Web, ils se sentiraient légitimes de se les approprier et ne se jugeraient donc pas coupables, par exemple, de copier-coller des informations tirées d'Internet en omettant les références nécessaires ou la demande de permission d'utiliser le matériel trouvé. Il est possible que les valeurs inhérentes au Web 2.0 (*le partage des idées, la collaboration, la construction d'un savoir collectif)* aient une influence sur eux et les portent à croire que les informations et les idées qu'ils trouvent sur le Web soient la propriété de la collectivité[22]. Plusieurs fonctions du numérique participent à l'amplification du potentiel de plagiat et de la falsification des documents académiques. C'est le cas de la fonction « *copier-coller* **»,** dont le moindre rédacteur ne pourrait plus se passer aujourd'hui. Tout comme le recours à Internet comme source d'information est devenu inévitable pour trouver rapidement une information, et ce, peu importe que l'on soit étudiant, professeur ou membre du personnel. On parle même aujourd'hui du réflexe « *Google* ». La facilité d'utilisation de la fonction « *copier-coller* », combinée à l'impression que la quantité phénoménale d'informations (*textes, codes, images, sons…)* disponibles via Internet appartient à tous, banalise le « *repiquage* » de matériel en ligne. Le problème n'est pas la fonction « *copier-coller* », mais l'absence, volontaire ou non, de références aux sources utilisées pour réaliser un travail.

Différentes études réalisées à propos des habitudes de travail des étudiants donnent une idée de l'ampleur du problème de la falsification et du plagiat numérique liés au « *copier-coller* ». En 2007, l'Université de Lyon a commandé une étude[23] afin d'évaluer les habitudes de ses étudiants à propos d'Internet. 1102 étudiants et 117 enseignants ont répondu à l'appel. De ce nombre, il s'est révélé que 79,7 % des étudiants ont avoué « *copier-coller* » des renseignements en provenance d'Internet sans référence aux sources; 9 professeurs sur 10 ont dit avoir déjà été confrontés au « *copié-collé* » sans référence aux sources.

---

[22] Beaudin-Lecours, M., Le Web 2.0, Bulletin Clic, Numéro 66 Janvier 2008 : http://clic.ntic.org/cgi-bin/aff.pl?page=article&id=2071

[23] Cette enquête peut être téléchargée à cette adresse : http://www.compilatio.net/files/sixdegres-univ-lyon_enquete-plagiat_sept07.pdf

Selon l'enquête, les étudiants copient-collent sans référence aux sources pour les raisons suivantes : *par facilité (59,7%); par manque de temps (34,8%); parce que tout le monde le fait (8,2%); parce que les profs ne voient pas la différence (3,6%); parce qu'il s'agit d'une pratique sans risque de sanction (2,2%)*[24].

Ainsi, *la facilité et le manque de temps* se détachent nettement comme principales motivations du « *copier-coller* » chez les étudiants. Les statistiques précédentes sur le comportement des étudiants avec Internet interpellent les institutions tout autant que les enseignants. Avec toute cette information disponible sur Internet, les enseignants sont aux prises avec l'impression, bien fondée, que beaucoup de cas de plagiat leur échappent parce que l'explosion de la production de connaissances et la quantité d'information en circulation sur le Web ont érodé leur sentiment de maîtriser, et de reconnaître, ce qui a été écrit sur leur matière, leur discipline, leur champ d'expertise...

D'autres questions peuvent également être soulevées : Les enseignants tiennent-ils compte de l'accessibilité de cette information dans leurs exigences pour les travaux? Comment les valeurs universitaires d'intégrité sont-elles rendues visibles? Comment la réglementation est-elle diffusée? Comment la formation aux compétences informationnelles et rédactionnelles est-elle offerte et les apprentissages réinvestis dans les différentes composantes d'un programme d'études? Les impacts du numérique sur la relation enseignant-étudiant et sur la production de nouveaux savoirs ? font-ils l'objet de discussion, de débats au sein de la communauté universitaire? …

Selon certains auteurs, tels que *Davidson et Goldberg (2009)*[25], l'Internet constitue la quatrième révolution de l'information (*les trois autres étant l'invention de l'écriture, l'invention du livre manuscrit et l'invention de l'imprimerie*). Le phénomène de la falsification et du plagiat numérique s'insère dans cette nouvelle ère de l'information et les actions posées pour l'enrayer doivent être prises en tenant compte de ce nouveau contexte.

---

[24] *Ibid, p. 32.*

[25] *Davidson, C.N. and Goldberg, D.T., 2009. The Future of Learning Institutions in a Digital Age. USA: The MIT Press.*

III.5. RECOMMANDATIONS POUR CONTRER LA FALSIFICATION ET LE PLAGIAT NUMERIQUE EN RDC

Pour contrer la falsification et le plagiat digital en RDC, exacerbé par l'avènement du numérique, la majorité des institutions congolaises doivent se doter d'une position institutionnelle qu'elles affichent clairement, parfois même sous forme de slogan. Elles doivent développer une ou des pages Internet propres à la falsification et au plagiat où on retrouve les formes que peut prendre le plagiat et la falsification des documents académiques, diverses informations, dont la réglementation et les sanctions possibles en cas de plagiat avéré; d'outils d'autoformation aux compétences informationnelles; des jeux informatifs, des témoignages relatifs à l'intégrité intellectuelle, et des recommandations pédagogiques à l'intention des enseignants…

Certaines doivent se doter d'un logiciel de détection de similitudes dans le texte. D'autres encore doivent exiger que tout certificat ou travail remis pour évaluation soit accompagné d'une attestation d'honnêteté ou l'on oblige leurs étudiants à réussir un quiz sur comment éviter les différentes formes de plagiat et de la falsification…

Dans tous les cas, les actions anti-plagiat et anti-falsification d'entreprises doivent viser la sensibilisation, la prévention, le traitement et/ou la sanction. La tendance actuelle consiste à considérer le plagiat et la falsification électronique comme un problème systémique qui exige une approche intégrée et une responsabilité partagée entre les divers membres de la communauté du secteur éducatif en RDC. Ainsi, nous nous joignons à La position de la professeure de l'Université de Genève, *Michelle Bergadàa*[26], qui propose sur son site Internet un projet intégré institutionnel :

[26] *Ce projet intégré a été créé par la Commission Éthique-Plagiat, dont nous avons déjà parlé, et peut être trouvé en ligne : http://responsable.unige.ch/index.php (faire dérouler la page pour trouver « Vers un projet intégré institutionnel »*

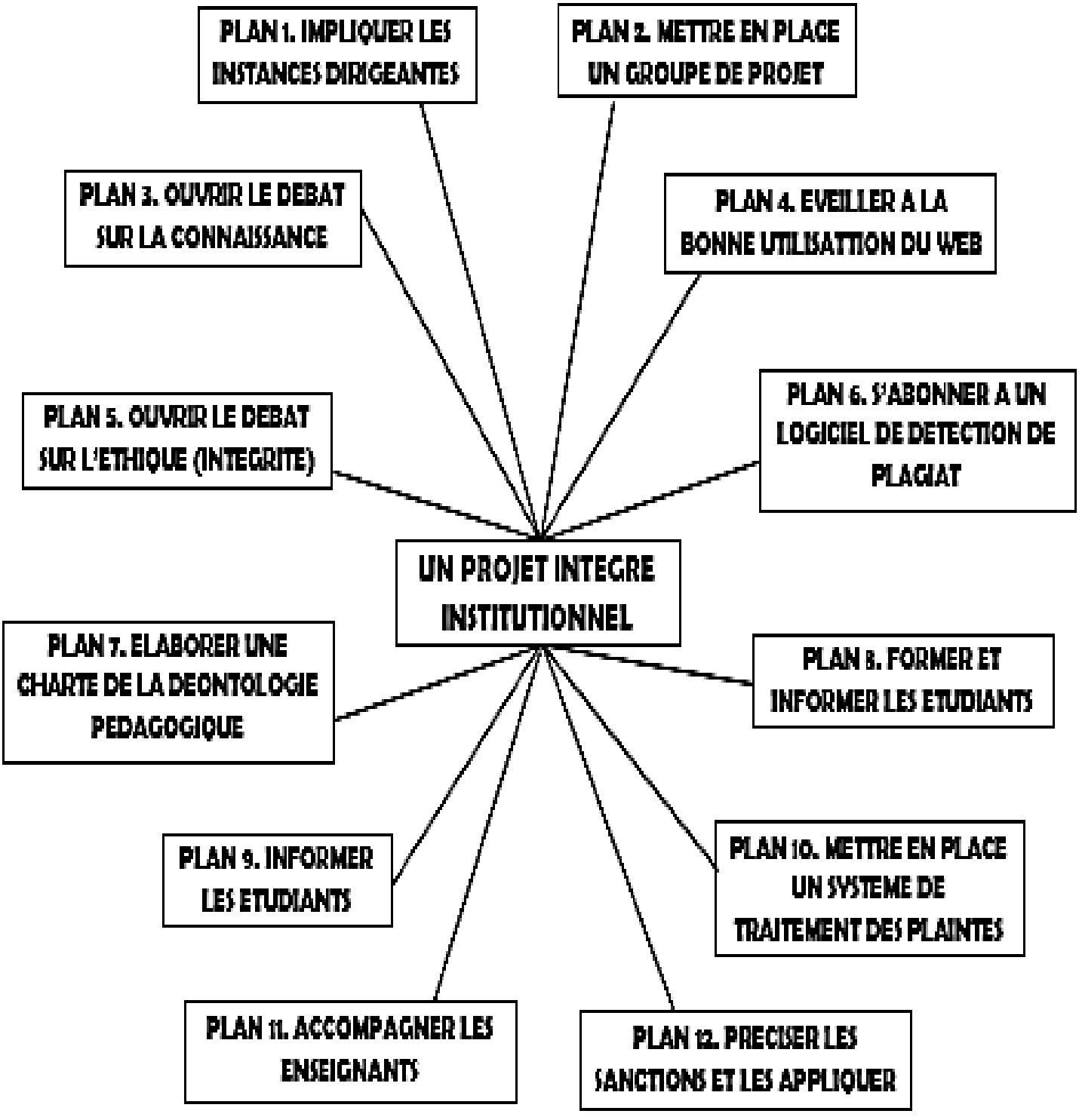

Illustration du projet intégré institutionnel de la professeure Michelle Bergadàa, qui a été appliqué, à divers degrés, par les universités de Genève, Lausanne et par l'Université catholique de Louvain.

Au Royaume-Uni, le Service d'intégrité académique (*Academic Integrity Service*) du Higher Education Academy (HEA) a produit en 2011 un rapport intitulé Policy Works[27]. On y trouve une série de recommandations pour traiter les pratiques académiques inacceptables dans l'enseignement supérieur.

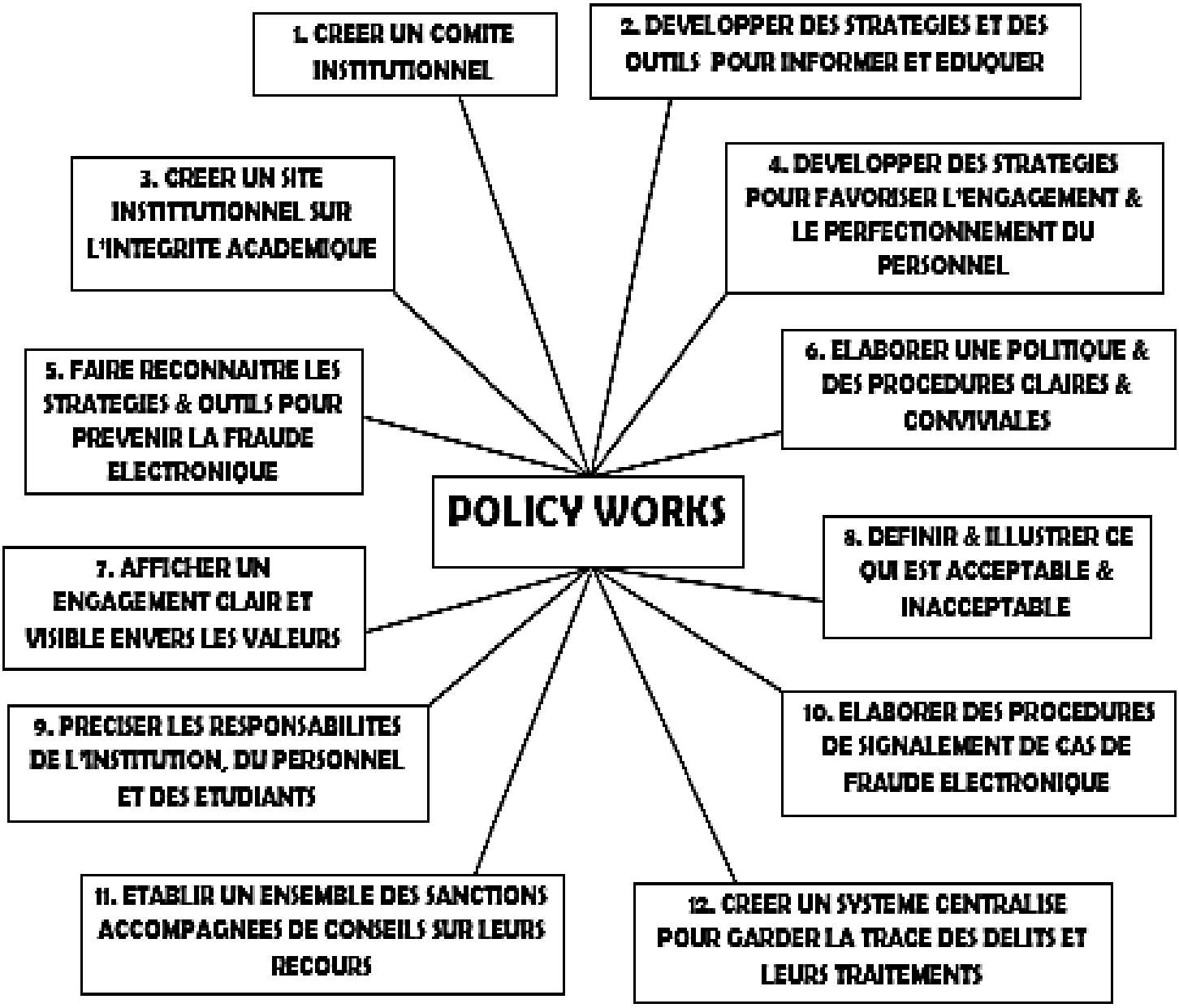

Illustration du rapport intitulé « Policy Works » du Service d'intégrité académique (HEA) Au Royaume-Uni.

---

[27] Policy works. Higher Education Academy (UK). 2011. Disponible à http://www.heacademy.ac.uk/ourwork/teachingandlearning/assessment/alldisplay?type=resources&newid=ourwork/academicintegrity/policy_works&site=york

CONCLUSION

En guise de notre conclusion, Les recommandations de l'HEA (*Higher Education Academy*) s'apparentent au projet intégré institutionnel de Madame Bergadàa. En fait, dans les deux propositions, on retrouve :

- la création d'un comité institutionnel ;
- l'implication de la haute direction des établissements universitaires ;
- l'information et la formation des étudiants ;
- la mise en place de procédures conviviales pour le signalement et le traitement de plaintes relatives au plagiat et un soutien aux enseignants dans leurs démarches ;
- un engagement clair et visible en matière d'intégrité intellectuelle ;
- le recours à un logiciel de détection de similitudes.

Le fait que les deux approches intégrées comprennent le recours à un logiciel de détection de similitudes dans le texte, cela doit pour autant encourager davantage les institutions congolaises à examiner plus en détail cet élément de lutte anti-plagiat et anti-falsification numérique.

Quant à la question posée au début de cet article, il est évident que l'hypothèse est affirmative en se rapportant à l'approche de l'HEA et de la Professeure BERGADAA Michelle, ce qui nous permet à notre tour de formuler les avertissements ci-après (*Au Gouvernement congolais*) :

- D'aider le Ministère de l'Enseignement Supérieur Universitaire et Recherche Scientifique à mettre au point une institution appropriée qui permettra et facilitera l'échange et le contrôle des documents académiques dans toute la République dans toutes ses dispositions ;
- De garantir la sécurité la plus fiable dans le but de protéger l'institution mise en place ;
- De doter cette institution du personnel de maintenance (IT) qualifié pour assurer l'entretien permanant du matériel informatique pour la durabilité des machines ; Equiper cette institution d'une connexion internet à haut débit pour permettre cette circulation des données ;
- De mettre en place un site web avec une sécurité plus fiable dans le but de protéger les informations mise en place…

BIBLIOGRAPHIE

1. **Abbas JABER**, « *Les infractions commises sur Internet* », Thèse, Université de Bourgogne, France, novembre 2007 ;
2. **ARCEP**, « *Étude sur le périmètre de la notion d'opérateur de communications électroniques* », Paris, 2007 ;
3. **Beaudin-Lecours, M**., « *Le Web 2.0* », Bulletin Clic, Numéro 66 Janvier 2008 : http://clic.ntic.org/cgi-bin/aff.pl?page=article&id=2071
4. Cette enquête peut être téléchargée à cette adresse : http://www.compilatio.net/files/sixdegres-univ-lyon_enquete-plagiat_sept07.pdf
5. **Davidson, C.N. and Goldberg, D.T.** « *The Future of Learning Institutions in a Digital Age* », USA: The MIT Press, 2009
6. **François-Bernard Huyghe**, « *Le cyberespace, nouvel enjeu stratégique* », émission Géopolitique, le débat sur RFI, 23 septembre 2012 ;
7. http://www.compilatio.net/files/sixdegres-sphinx_enquete-plagiat_fev06.pdf
8. **Jacques HALLAK** et **Muriel Poisson**, « *Écoles corrompues, universités corrompues : que faire ?* », Broché – 2009 ;
9. **Jean-Denis Garo**, « *Mon papa travaille dans l'Informatique et les Télécoms* », Paris, 2007 ;
10. **Krafft, J,** « *Profiting in the Age of Broadband: Lessons and New Considerations. Technological Forecasting & Social Change* », Vol. 77, p. 265-278 ;
11. **KUMABA M. Wutibaal,** « *L'ONU et la diplomatie des conflits : le cas de la République démocratique du Congo* », Le Harmattan 2012, 417p.
12. **M.J. ALULA LIOKE NYOTA**, « *Aperçu historique de l'enseignement supérieur et universitaire* », Kinshasa, 2014 ;
13. **McKinsey & Company,** « *Impact d'internet sur l'économie française ; comment internet transforme notre pays du ministère de l'économie* », 45 pages, 2011 ;

14. **Mohamed CHAWKI,** « *Le droit pénal à l'épreuve de la cybercriminalité* », Thèse, Université Lyon III, France, septembre 2006.

15. **MOPONDI BENDEKO MBUMBU**, « *Des objectifs de l'enseignement à la formation des enseignants en république démocratique du Congo* », Docteur en Didactique des Mathématiques, Professeur Associé, U.P.N.-Kinshasa ;

16. **Myriam QUEMENER et Joël Ferry**, « *Cybercriminalité : Défi mondial et réponses* » - 2ème édition, Perpignan, Economica, 9 mars 2009, 308 p.

17. **Nations Unies,** « *Progrès accomplis dans la mise en œuvre et le suivi des résultats du Sommet mondial sur la société de l'information aux niveaux régional et international, Conseil économique et social*, Genève, juillet 2013 ;

18. Policy works. Higher Education Academy (UK). 2011. Disponible à http://www.heacademy.ac.uk/ourwork/teachingandlearning/assessment/alldisplay?type=resources&newid=ourwork/academicintegrity/policy_works&site=york

19. **Rodolphe Monnet et Franck FRANCHIN,** « *Le business de la cybercriminalité* », Hermès - Lavoisier, avril 2005

20. **Yves Jeanneret**, « *Y a-t-il vraiment des technologies de l'information ?* », Presses Universitaires du Septentrion, 2007 (ISBN 2757400193) ;