Université Catholique du Graben
Centre de Recherches Interdisciplinaires du Graben
Gouvernance, Paix et Développement
ISSN : 3008-1211 e-ISSN : 3008-122X

PIRIG 32, septembre 2025, pp. 177 - 191
https://doi.org/10.57988/crig-2113
N° du dépôt légal : 11108-2002-38

L'abc d'une technophanie numérique assumée

Rafiki KAMBALE MWENGESYALI et Gaston KAMBALE MALULA*

Résumé

Les opportunités innovatrices et alléchantes offertes à temps réel par le modernisme numérique condamnent de plus en plus et à une vitesse vertigineuse les modes de vie d'hier à demeurer des simples repères historico-nostalgiques. Tout s'embarque par et dans la technologie numérique de telle sorte que le traditionalisme standard s'estompe sans préavis. D'où la nécessité et l'impératif pour les utilisateurs non aguerris au numérique de se recycler à ses exigences, sous peine de demeurer des intellectuels obsolètes. Dans cet article, nous soulignons quelques notions susceptibles d'aider à répondre à cet impératif à l'heure actuelle du développement inédit de la science et de la technique.

Mots-clés : Technophanie, Versatilité, Matière calculée et Mode de vie.

Abstract

The enticing and innovative opportunities offered in real time by digital modernism are increasingly and rapidly relegating yesterday's ways of life to mere historical and nostalgic reference points. Everything is now shaped by and embedded within digital technology, to the extent that traditional standards are fading without warning. Hence the urgent need-and even obligation-for those unfamiliar with digital tools to retrain and adapt to its demands, or risk becoming obsolete intellectuals. In this article, we highlight a few key concepts that may help address this imperative in an era marked by marked by unprecedented advancements in science and technology.

Keywords: Technophany, Versatility, Calculated matter, and Lifestyle.

Introduction

Par technophanie[1] numérique, il faut entendre la manifestation vertigineuse de l'avènement de l'ordinateur dans tous les méandres de la vie. En effet, à l'heure actuelle, chacun peut observer, depuis son ordinateur ou son Smartphone, le flot d'innovations désormais disponibles : applications

* Enseignants à l'IBTP - Butembo

[1] Fait référence à « épi-phanie », concept relatif au « temps de Noël chrétien » pendant lequel le petit Jésus né s'était « manifesté » aux peuples du monde entier symbolisé par les Mages pour Le visiter. La ‘‘technophanie’’, c'est, selon notre entendement, la manifestation vertigineuse de l'avènement de l'ordinateur avec ce qu'il implique.

de reconnaissance musicale, films, vidéos, informations, etc. Le logiciel qui « 'dévore le monde', l'information qui se trouve à présent partout : dans nos réfrigérateurs, nos voitures, nos trains, nos magasins, … et même dans nos brosses à dents ou nos fourchettes » (Babinet, 2014, p.78, p.39) est l'œuvre de l'ordinateur, lequel est au cœur d'une thaumaturgie sans pareil et tributaire des métamorphoses qualitatives, quantitatives, économiques et de *design* effectuées sur le tout premier ordinateur[2]. Grâce à sa large disponibilité par ses dernières versions (Desktops, Laptops, Tablettes, iPhones et Smartphones), à sa non-réservation aux seuls endroits spécifiques, à sa miniaturisation, à son omniprésence sur la table ou dans les poches des intellectuels avérés, accroissement de sa mémoire, à sa vertigineuse vitesse à traiter les données ainsi qu'à sa distribution adaptée à toutes les bourses, la « machine intelligente »[3] et *supra* logique que l'ordinateur est devenu contraignant et fatal.

Maximiser ses acquis, dans le monde d'aujourd'hui et, surtout, dans le monde de demain qui s'annonce indubitablement informatique, devient alors un impératif. Que faisons-nous donc pour nous inscrire dans cette logique du monde numérique de demain ? Du fait que le numérisme a su mettre la parole dans la bouche et la tête des innocents, des naïfs et des illettrés, quels garde-fous est-on en train de placer pour se prévenir d'éventuels dérapages ? Est-on de ceux qui possèdent des appareils numériques, le téléphone intelligent en l'occurrence, comme simple fait de mode ou en profitons-nous au maximum, vu que la technologie numérique est désormais tout sauf rien ? Ce

[2] L'ENIAC (Electronic Numerical Integrator Analyzer and Computer) de John ECKERT et John W. MAUCHLY). On dit de lui qu'il pesait plusieurs tonnes et était très encombrant.

[3] Pas dans le sens que l'ordinateur pourrait, à lui seul, prendre une initiative pensante. L'activité pensante effectuée par l'ordinateur est, jusqu'à preuve du contraire, la conséquence d'une série d'instructions programmées par l'homme. Autant dire que, sans l'intervention de l'homme, l'ordinateur reste un idiot. Autrement dit, « si l'ordinateur produit effectivement des propositions accessibles à l'entendement humain, il n'est pas 'intelligent' dans le sens où il ne 'comprend rien de ce qu'il fait ». LELEU-MERVIEL Sylvie, « Les désarrois des 'Maîtres du sens' à l'ère numérique », dans *Créer du sens à l'ère numérique.*H_2PTM_{03}, Hermès, 2003, p.20. Pour le Professeur MVUEZOLO MIKEMBI Ignace, « l'homme, par son intelligence intuitive, par sa créativité, par sa capacité éthique, par son ouverture à la transcendance, est absolument irréductible à toute machine à penser ». Cf. « Les enjeux d'Internet », dans NDUMBA Y'Oole L'Ifefo Georges (dir.), *Sociétés africaines et nouvelles technologies. Enjeux existentiels.* Revue Philosophique de Kinshasa / Faculté de Philosophie, Vol. n°23-24 (janvier-décembre 1999), p.87.

questionnement nous aidera à faire une analyse phénoménologique du phénomène numérique afin d'envisager des solutions (pédagogiques) au problème que pose celui-ci pour un destin tant soit peu assumé.

Le fond méthodologique de notre réflexion est l'approche constructiviste. Celle-ci consiste, à partir de quelques allégations choisies à volonté chez des auteurs, à construire un argumentaire dissuasif.

Deux grands points constituent l'ossature de l'article : la versatilité de la technologie numérique et le mode de vie d'être du numérique. Ce dernier, en tant que station fondamentale de notre propos, sera, à son tour, subdivisé en quatre sous-points, à savoir les fondamentaux de l'éducation de base, la langue du numérique, l'éducation technique au numérisme et l'éducation à la sécurité numérique. Ce dernier sous-point s'articulera autour de trois thèmes : d'abord, l'éducation relative au système d'exploitation, ensuite l'éducation liée aux faits ''rupturistes'' et, enfin, une gamme d'astuces auxquelles on peut recourir.

1. Versatilité du phénomène numérique

Versatilité (Vial, 2012, p.229-232), quid ? Par l'expression ''versatilité du phénomène numérique'', nous entendons simplement le fait que ce phénomène est, dans son essence, très instable. Comment cela ? Un jour de septembre 1947, dans l'équipe qui travaille sur le « Harvard Mark II »[4] sous la direction de Howard Aiken, le calculateur électromécanique qui succède au très médiatique Harvard Mark I, la présence d'une mite dans le relais 70 du panneau F provoque l'arrêt de la machine, sous les yeux incrédules de Grace Hopper. À l'aide d'une pince à épiler, Grace déloge le papillon de nuit le plus célèbre de l'histoire informatique et le colle dans le journal de laboratoire sous le titre « premier cas avéré de *bug* » (en anglais, *bug* signifie insecte).

Quoique Thomas Edison emploie déjà le mot dans ses notes pour désigner un défaut, Grace Hopper est la première à en faire un usage informatique. Au départ, il s'agit seulement d'un insecte qui grille dans un relais, provoquant une panne générale de la machine. Le terme devient néanmoins populaire et s'impose rapidement dans le domaine pour désigner toute erreur de conception à l'origine d'un dysfonctionnement dans un

[4] Une des machines de la première génération des ordinateurs.

programme informatique. La notion de *debugging* (débogage) introduite par Grace Hopper prend alors tout son sens : il s'agit de rechercher dans le code informatique l'insecte logique qui fait planter la machine. Dès lors, ce qui est arrivé au Harvard Mark II ne cessera d'arriver à tous les ordinateurs qui lui succèderont parce qu'un ordinateur ne peut pas vivre sans *bugs,* sans un seul défaut de performance (Vial, 2012, p.229).

En effet, quelle que soit la compétence des auteurs des programmes informatiques, ceux-ci ne sont jamais complètement maîtrisables *a priori* par un cerveau humain. Avant qu'un programme soit pleinement opérationnel, il faut le faire exécuter de nombreuses fois par la machine afin de vérifier ses comportements dans les moindres situations et rectifier les inévitables lacunes. Aucun programmeur au monde, quel que soit son génie, n'est capable d'écrire un programme qui fonctionne parfaitement, du premier coup, sans *bugs*. C'est pourquoi, il y a toujours de nombreux tests et débogages à faire avant de lancer un logiciel, une application ou un site *Web*, parce qu'il y a toujours des comportements qui n'ont pas pu être anticipés. Et c'est la raison pour laquelle les informaticiens numérotent toujours les versions de leurs programmes avec beaucoup de prudence, ne consentant à accorder le titre d'une version à un logiciel (1.0, par exemple) que lorsque celui-ci a fait l'objet de nombreuses versions préalables, longuement testées et vérifiées. Or, malgré cela, il y a toujours des failles possibles dans le code d'un programme, rendant régulièrement nécessaires des mises à jour correctives de sécurité. Il est donc impossible de coder sans engendrer des bugs, même si, après coup, ils peuvent tous être corrigés. Le *bug* est donc consubstantiel à la matière calculée qui caractérise le système informatique. Autrement dit, la matière numérique est nécessairement une matière qui achoppe, qui trébuche, qui chute. On dit d'ailleurs, lorsqu'il est victime d'un bug, qu'un serveur est *down* ou qu'un site est planté. Et ce n'est pas seulement vrai pour le développeur informaticien. Cela est également la règle dans les domaines de recherche certains étant évidemment plus exposés que d'autres. « Pour mettre au point son ampoule électrique, Thomas Edison, avait par exemple dû passer par dix-milles essais infructueux » (Nkombe, 2000, p.99).

Une fois entré dans son cycle de vie et mis entre les mains d'un usager, un programme finit toujours, à un moment ou à un autre, par produire un *bug*. Par exemple, les utilisateurs du système d'exploitation Windows de Microsoft ont tous connu, au moins une fois, le fameux *bug* connu sous le

nom de *Blue Screen of Death* (Ecran Bleu de la Mort ») que le système affiche lorsqu'il rencontre une erreur critique. De même, quel que soit le système utilisé, il est arrivé à tout le monde, au moins une fois, d'être contraint de redémarrer sa machine, de relancer une application ou de recommencer une action. Sur un Smartphone de dernier cri, il arrive de temps en temps qu'une application se referme brutalement, sans raison apparente, ou qu'il ne soit pas possible de décrocher lorsqu'on reçoit un appel entrant, alors même que notre doigt effectue le bon geste. Comme si, dans la matière calculée, il existait une tendance structurelle au bug (Vial, 2012, p.231).

Certes, certains programmes sont connus pour être plus stables que d'autres. Mais, en définitive, quel que soit le constructeur ou le développeur, il y aura toujours, dans un produit informatisé, une tendance irréductible à l'instabilité, sans compter les anomalies issues d'actes de malveillance comme les virus. Cette instabilité, engendrant le stress informatique, fait partie de la nouvelle culture numérique avec laquelle, depuis quelques années, nous avons appris à vivre. Habitués aux aléas fonctionnels de nos ordinateurs, nous savons désormais que « ça peut planter ». Par conséquent, vivre dans la culture numérique, c'est vivre avec une matière instable, à laquelle nous confions tout, mais à laquelle nous ne pouvons pas totalement faire confiance. C'est aujourd'hui un impératif d'adopter un certain mode de vie face au numérique en vue d'une intégration assumée dans le monde actuel.

2. Mode de vie du numérique

Il y a toute une kyrielle d'aspects du mode d'être de la technologie numérique. Symboliquement ou à titre exemplatif, nous nous limitons à quelques quatre d'entre eux, en commençant par les fondamentaux de l'éducation de base.

2.1. Fondamentaux de l'éducation de base

De son caractère complémentaire à toutes les technologies qui ont existé auparavant, la technologie numérique fait sauter les étapes chronologiques de la formation humaine de base. Avec seulement le numérique comme savoir technologique d'usage, des générations actuelles et futures risquent de ne pas maîtriser les fondamentaux de l'éducation de base : lire, écrire, calculer et déduire. La technologie numérique *via* le téléphone portable a tout simplifié outre mesure. Pour signifier, par exemple, que quelqu'un est mort,

on lui colle un *sticker* correspondant à un texte contextuel ; la bonne humeur ou les autres sentiments ayant leurs *stickers*, lesquels leur correspondent. D'où l'usage du concept ''*génération androïde*'' : l'ensemble de toutes ces personnes nées sous le boom numérique avec le téléphone portable, puis le smartphone en mains, en poche ou dans le sac, à l'école comme à l'église, au marché comme au lieu de deuil, au lit comme en douche, etc. Vous voulez abrutir votre enfant vis-à-vis de tous les autres devoirs pour la vie ? Laissez à sa disposition un « Androïde ». Les enfants pour qui l'amusement fait partie intégrante de leur être, sont plus captivés que quiconque en face d'un téléphone intelligent fonctionnel ; le caractère ludique ou jouable du téléphone coïncidant parfaitement avec leur nature.

Voilà ce qui nous fait dire, sans ambages, que les traditionnels éducateurs que sont les parents et les enseignants ont du pain sur la planche. Ils ont là un nouveau matériel didactique, d'autres objectifs opérationnels à atteindre afin que les apprenants, non assez doués en discernement, ne s'adonnent pas au numérique jusqu'à étouffer tous les aspects de leur apprentissage. En effet, à force d'être embarqués et emballés par la technophanie numérique, ils courent le grand risque d'oublier qu'il faut la consommer avec les bonnes références d'une éducation basique comprenant la maîtrise de la lecture, de l'écriture, de la mathématique et de la déduction. Face aux interfaces numériques qui nous tombent par-dessus nos têtes, leur manipulation exige la maîtrise de l'abc d'une éducation de base digne, sans laquelle l'ordinateur ou le portable deviendra davantage un labyrinthe. Par contre, en adoptant le numérique avec les notions de base bien aiguisées, l'on est un probable expert du domaine, susceptible de profiter au maximum du caractère thaumaturgique de la matière calculée. Le monde se configure de plus en plus au numérique de sorte que, demain, tous les esprits sans formation adéquate s'élimineront eux-mêmes sur le champ utile parce que n'ayant rien à offrir de ce point de vue. Seuls les visionnaires, les critiques objectifs et les prospectivistes peuvent saisir la balle au bond.

À ces fondamentaux de l'éducation de base qu'il faut maîtriser pour s'approprier et se servir adéquatement de la technologie numérique, il convient d'ajouter la langue de l'informatique qui est l'anglais.

2.2. Anglais technique au cœur du numérique

L'appropriation du numérique doit particulièrement tenir compte de l'apprentissage de l'anglais. Telle est la langue numérique qui, de plus en

plus, s'impose. De simples catalogues des applications ou logiciels jusqu'à leurs codes sources en passant par des messages-guides, tout cela est conçu en anglais. Celui qui ne la maîtrise pas s'en étonne.

Argumentant vingt ans plus tôt sur les enjeux d'Internet, sève même de la technologie numérique, Mvuezolo le voyait déjà comme dans les jumelles. Pour lui, « on ne doit pas (…) perdre de vue que l'accès au réseau nécessite l'apprentissage de l'anglais puisque 80 à 90% de l'information offerte est en langue anglaise » (Mvuezolo, 1999, p.86). Il avait ainsi gonflé la liste de ceux qui étaient convaincus de ce préalable, dont Nkombe Oleko et Van Parys qui, respectivement, avaient allégué : « Pour de milliards d'individus à travers le monde, l'accès à la modernité s'identifie au mode américain de vie et de pensée. Cette hégémonie culturelle s'appuie sur trois facteurs : la langue, les universités et les médias » (Nkombe, 2000, p.93) ; « le capital humain – travail hautement qualifié – devient de plus en plus mobile, en particulier dans les pays où l'anglais est largement répandu parmi ses travailleurs hautement qualifiés, et leurs familles. À mesure que l'anglais se diffuse davantage comme *lingua franca* international, le pouvoir d'attraction différentiel des pays de langue anglaise sur le capital humain mondial ne cesse d'augmenter » (Van Parys, 1999, p.152 et 153).

Nos populations doivent donc acquérir et l'alphabétisation ordinaire et l'alphabétisation de l'informatique. Ils doivent, en outre, intégrer l'éducation aux technologies numériques et l'informatique dans les programmes de cours de sorte qu'elle devienne une nouvelle culture (Mweze, 1999, p.186 et 187). Il faut le vivre et, surtout, en vivre. Le contraire, c'est un début vertigineux vers le déphasage vis-à-vis des exigences du monde actuel. L'anglais comme langue numérique étant jusque-là acquis, faut-il encore se tourner vers l'éducation technique proprement dite.

2.3. Éducation technique numérique

À la disparition des lettres (missives) sous le format de papier, on ne cesse de voir avec quel complexe d'infériorité ceux qui ont ignoré l'alphabétisation ordinaire sollicitent des aides devant des interfaces de leurs propres portables. Soit pour déduire la logique d'envoi d'un simple message électronique, soit pour crier secours face aux difficultés qu'ils rencontrent en matière de retrait du *cash* virtuel, soit encore pour s'auto-guider dans les méandres de services qu'offrent leurs propres téléphones. Autrement dit, l'on

achète des téléphones dont le coût est disproportionnel au niveau économique pour les sous-utiliser, sinon pour en disposer comme un simple fait de mode. De nombreux usagers du numérique se nivellent vers le bas : soit, pour avoir relativisé de gré ou de force l'éducation de base ; soit du fait qu'il semble trop tard pour eux de s'auto-engendrer et revenir à l'âge psychologique d'apprentissage de base. Vont-ils souhaiter cette contre-nature à leur descendance ? Non. En effet, la vie foncièrement numérique de demain exigera à chacun de s'imprégner des préalables de la technologie numérique sous peine de demeurer un éternel exécutant à côté de ceux qui piloteront réellement le monde grâce à leur formation scientifico-technique avérée.

Par ailleurs, au regard du fait que nous faisons face, jour après jour, à un nouveau vocabulaire d'abréviations, néologismes et anglicismes relatifs à la technologie numérique, le risque est grand de subir le destin. Qui ne se demande ce que signifient, de nos jours, cyber (cybercafé, cyberespace, cyber crimes ou cybercriminalité), surfer, méga, octet, pilotes, fichier, logiciel, routeur, virtuel, *Data, Big Data*, télécharger, etc. ? Il n'y a pas que ces concepts relatifs au *software*. L'autre paire de manche de l'informatique qu'est le *hardware*, en a autant : des concepts techniques à maîtriser pour espérer s'imprégner du langage numérique dans toute son intégrité. Pour emprunter la formule de Dominique Mweze, « étant donné que les concepts en usage dans les Nouvelles Technologies de l'Information et de la Communication (NTIC) ne sont pas attestables, mal formés au regard de la grammaire qui leur sert de référence, ils sont inaptes à communiquer le savoir à ceux qui ne sont pas initiés » (Mweze, 1999, p.182). Il suffit seulement de visiter les réseaux sociaux avec un intérêt particulier pour s'en rendre compte et juger. Tandis que les savants y exhibent le niveau de leur scientificité, les humoristes y pompent leurs blagues récréatives et parfois instructives, les marqueteurs, eux, y trouvent un outil de la taille de leur entendement. Les médiocres, opportunistes ou parvenus, par contre, y font preuve de médiocrité et de barbarie en s'y caractérisant par les invectives, les caricatures, le fanatisme, l'exposition de la vie privée d'autrui, le refoulement psychologique qui laisse à désirer et tout ce qui est *fakes news* ou *intox*. À chacun donc de jouer, étant donné que la balle est bel et bien dans le camp de tous selon la même égalité de chance ! Aux éducateurs de jouer davantage parce qu'ils sont censés être doublement aguerris : vis-à-vis des apprenants vides numériquement et face à tous ceux qui en sont numériquement outillés n'importe comment.

Ceux qui, du numérique, ont fait leur outil privilégié, et ceux qui, surtout, se sont déjà imposé une certaine éducation numérique, ont intérêt à percer jusque dans l'éducation à la sécurité informatique. Pour beaucoup d'entreprises, celle-ci apparaît comme « un élément absolument vital » (Bloch et al., 2007, p.123).

2.4. Éducation à la sécurité numérique

En cette matière, nous nous limitons aux allégations de Bloch et Wolfugel. Dans leur livre consacré à la sécurité informatique, les auteurs évoquent les causes des risques inhérents à tout système informatique ainsi que les moyens de s'en protéger.

Au regard du fait réel que l'administrateur et le responsable informatique affrontent une insécurité informatique protéiforme et envahissante, qui menace tant les données que les applications de l'entreprise : virus, attaques par le réseau, tromperie sur le Web, etc., les auteurs proposent des outils pour y faire face : 1) Outils techniques de la sécurité : définir les risques et objets à protéger, identifier et authentifier, empêcher les intrusions, défense en profondeur ; 2) Outils organisationnels de la sécurité : abandonner les utilisateurs inexpérimentés aux requins, sauvegarder données et documents, vérifier les dispositifs de sécurité ; 3) Outil managérial de la sécurité : construire une politique de sécurité applicable verticalement et horizontalement dans l'entreprise.

Par ailleurs, les auteurs suggèrent de comprendre d'abord le rôle et le mode opératoire des menaces et de les replacer dans le cadre d'une politique de sécurité efficace. On devra, pour cela, garder en tête les principes qui animent tout système d'information et chasser de dangereuses idées reçues. Les deux techniciens poursuivent en offrant au professionnel consciencieux des principes clairs et une méthode rigoureuse pour concevoir une véritable politique de sécurité informatique.

S'agissant des risques en informatique, Bloch et Wolfugel vont plus loin en commençant par prévenir qu'il n'y a pas de métier sans risques. Détecter leurs zones et comment les éviter ou les prévenir, tel est déjà la clé de réussite de tout projet, informatique surtout. Lorsque les risques sont là, il faut les analyser afin de limiter leur nuisance. Cette étape d'analyse de risques consiste, dans le concret, à répertorier les différents risques encourus, à estimer leur probabilité et, enfin, à étudier leur impact sur l'ensemble du

système. Cela conduira à estimer le coût des dommages qu'une menace causerait (par exemple, attaque sur un serveur ou détérioration des données vitales pour l'entreprise). C'est ainsi qu'ils conseillent de dresser un tableau des risques et de leur potentialité, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonnés selon un barème à définir. Par exemple : 1) Risque sans objet (ou improbable) : la menace n'a pas lieu d'être ; 2) Risque faible : la menace a peu de chance de se produire ; 3) Risque moyen : la menace est réelle ; et, enfin, 4) Risque haut : la menace a de grandes chances de se produire. D'où une gamme d'astuces à appliquer pour espérer amoindrir les dommages informatiques.

2.5. Astuces pour faire du numérique une technologie du destin voulu

Nous retenons, parmi tant d'autres, des astuces techniques, préventives et juridiques.

2.5.1. Astuces techniques

Il n'y a pas de méthode unique de protéger correctement l'ordinateur contre les attaques parce que les programmes envahissants évoluent avec le temps en devenant de plus en plus sophistiqués, pour attaquer même les ordinateurs ayant les meilleurs systèmes de défense du monde. La protection technique d'un système est à multiples facettes. On peut protéger son système en utilisant une des méthodes suivantes : l'installation d'un antivirus, l'utilisation des pare-feu (*firewalls*), s'assurer que les seules personnes autorisées accèdent au système, profiter de la technique de cryptage des données par un antivirus, l'authentification, l'utilisation de la cryptographie, etc.

Un antivirus peut être acheté pour protéger le système d'exploitation contre les attaques des virus informatiques. Le niveau de protection varie en proportion de l'importance des données. Par exemple, les données médicales de la clinique de l'Université recevront une protection supérieure par rapport aux programmes écrits par les étudiants de L2 dans un de leurs cours de programmation. Car, les données de la clinique, une fois perdues, seront difficilement reconstituées. Mais, il est très utile de se souvenir que peu après qu'un antivirus est sur le marché, ceux qui créent des virus cherchent les moyens de les contrecarrer. Seul l'antivirus le plus à jour pourra être en mesure de dénicher les virus les plus récents.

Un ‘pare-feu’ est un ensemble de *hardware* et/ou de *software* conçus pour protéger un système en déguisant son adresse IP contre les outsiders ou les personnes étrangères n’ayant aucune autorisation d’accès à ce système. Un pare-feu se situe entre l’Internet et le réseau. Les tâches typiques d’un pare-feu sur un réseau consistent à enregistrer toutes les activités accédant à l’Internet, maintenir le contrôle d’accès sur la base de l’adresse IP du récepteur ou de l’expéditeur, maintenir le contrôle d’accès sur la base du service demandé à votre réseau, masquer le réseau interne contre des personnes non autorisées cherchant à avoir des informations sur votre réseau.

‘L’authentification’ consiste à vérifier si la personne essayant d’accéder à un système est autorisée à le faire. Souvent, cela est implémenté par l’utilisation d’un mot de passe. S’il n’est pas connu, on n’aura pas accès au système. L’utilisation d’un bon mot de passe et la formation des utilisateurs est la technique la plus élémentaire mais, parfois, la plus importante pour protéger les investissements en logiciels et matériels informatiques. Cependant, ceci n’est pas toujours facile à implémenter. Un bon mot de passe doit être inhabituel, inoubliable et changé souvent tous les trente ou quatre-vingt-dix jours. Selon l’idéal, il doit être une combinaison de lettres et des chiffres et, en plus, il doit être assez long.

Une autre façon de protéger les données est d’utiliser la cryptographie. Il s’agit d’écrire les données sous forme de codes secrets connus seulement de l’utilisateur et d’autres personnes pouvant les consulter.

Il y a également l’auto-pédagogie. En effet, des articles et liens en rapport avec la cybercriminalité sont sur le Net grâce auxquels on peut se perfectionner comme autodidacte en matière de sécurité et éthique informatique.

2.5.2. Astuces préventives

Ainsi que l’adjectif en épuise le sens (Pillou et al., 2011, p.38), il est ici question de répertorier les différents risques encourus, d’estimer leur probabilité et, enfin, d’étudier leur impact dans le monde informatique. À ce sujet, la meilleure approche pour analyser l’impact d’une menace consiste à estimer le coût des dommages qu’elle causerait (par exemple attaque sur un serveur ou détérioration des données vitales pour l’entreprise).

La panne d’un système informatique peut causer une perte de productivité et d’argent, voire des pertes matérielles ou humaines dans certains cas

critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement (faute) d'une des composantes du système d'information et de prévoir des moyens et mesures appropriées.

Enfin, une 'contre-mesure' représente l'ensemble d'actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques, mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

2.5.3. Astuces juridiques

L'aspect juridique (Cf. Google avec Cybercriminalité comme mot de recherche) de la sécurité informatique est à attribuer, dans le temps, à la Convention sur la Cybercriminalité du 23 novembre 2001 adoptée par les pays membres du Conseil de l'Europe ainsi que les Etats-Unis, le Canada, le Japon et l'Afrique du Sud. Ceux-ci ont adopté la Convention sur la cybercriminalité, aboutissement d'un long processus de négociations (vingt-sept versions antérieures et quatre années de négociations officielles). Il s'agit d'une convention pénale à vocation internationale destinée à lutter contre le cyber crime.

La Convention sur la cybercriminalité de 2001 poursuit trois objectifs déterminés : l'harmonisation des législations des Etats signataires, la modernisation de ces législations, notamment en matière procédurale ; et l'amélioration de la coopération internationale en matière d'extradition et d'entraide répressive.

Le premier axe est l'harmonisation des législations nationales en ce qui concerne la définition des infractions répertoriées par la Convention. Il s'agit donc d'incriminer quatre séries d'infraction qui sont : 1) Les infractions informatiques : falsification et fraude informatique ; 2) Les infractions de contenu : la pornographie enfantine. Le protocole additionnel inclut la propagation *via* Internet d'idées racistes et xénophobes ; 3) Les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le partage non autorisé *via* Internet des œuvres protégées ; 4) Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données ou des systèmes.

Ensuite, le deuxième axe, d'ordre procédural, définit les moyens d'enquête et de poursuite pénale les mieux adaptés à la mondialisation du réseau Internet. La Convention prévoit des règles pour garantir les droits des individus, mais aussi pour faciliter la conduite d'enquête. En ce sens, on peut citer, entre autres : les règles régissant la conservation des données stockées ; la conservation et la divulgation rapide des données relatives au trafic ; la perquisition des systèmes informatiques ; la saisie de données informatiques ; la collecte en temps réel des données relatives au trafic ; et, enfin, l'interception de données relatives au contenu.

Enfin, le troisième axe concerne la mise en place d'un système rapide et efficace de coopération internationale. À côté des formes traditionnelles de coopération pénale internationale prévues, notamment par les Conventions européennes d'extradition et d'entraide judiciaire, la Convention sur la cybercriminalité prévoit des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention. Ces conditions sont exigées afin que les autorités judiciaires et les services de police d'un Etat membre puissent agir pour le compte d'un autre Etat dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières. En outre, toute donnée obtenue devrait être rapidement communiquée à l'État intéressé.

Sans doute, ce texte international constitue un complément indispensable aux lois nationales pour contenir le phénomène de cette nouvelle criminalité « caméléon » dont on ne connaît pas encore – du moins avec certitude – toutes « les couleurs » et les menaces. Plusieurs années plus tard, c'est alors qu'on sent que certains Etats commencent à inclure le numérique dans leur juridiction. Etant donné que la RDC dispose déjà d'un code en cette matière, on est averti. « Le droit a-t-il ignoré l'informatique »[5], comme se demandait Marie-Charlotte Roques-Bonnet ? La réponse c'est non.

Conclusion

Ayant porté sur l'abc d'une technophanie numérique assumée, cet article est parti de l'évidence que la technologie numérique portée par l'ordinateur s'est imposée à tous les âges. Tout le monde y trouve sa part, tout s'y arrime, et sa vertigineuse propagation augure un futur indubitablement numérisé.

[5] Livre paru en 2010 aux éditions Michalon.

D'où deux camps constitués : celui des aguerris à ladite technologie et l'autre, celui des amateurs. Tandis que, pour les premiers, le numérique est tout sauf rien parce qu'ils en disposent des atouts de consommation intégrale et maximale ; pour les autres, plus nombreux d'ailleurs, il apparaît, par contre, comme un simple fait de mode. Ce qui devient un danger latent.

Afin que, pour ces derniers, le numérique devienne une chance, un certain mode de vie mérite d'être adopté, constitué notamment de la maîtrise des fondamentaux de la formation de base que sont : lire, écrire, calculer et déduire, l'anglais technique en tant que langue technique, l'éducation technique elle-même et, enfin, l'éducation à la sécurité informatique.

Dans ce sens précis où le numérique vient, comme une écharde, s'improviser dans les traditionnelles actions éducatives, les enseignants de carrière ont là un matériel didactique à maîtriser pour maintenir leur hégémonie éducative sur leurs apprenants. Leur tâche consistera à appliquer les fondamentaux de l'éducation de base aux méandres de la technologie de l'heure pour former des experts de la technologie du moment. Du fait que nous sommes devenus des « prisonniers de la virtualité », seuls les experts en sont potentiellement les privilégiés.

Références bibliographiques

Ouvrages

BABINET Gilles*, L'ère numérique, Un nouvel âge de l'humanité,* Paris, Éd. Le Passeur, 2014.

BLOCH Laurent et WOLFUGEL Christophe, *Sécurité informatique. Principe et méthode*, Paris, Ed. Eyrolles, 2007, 262p.

EMPIRICUS Sextus, *Esquisses pyrrhoniennes*, I, Paris, Seuil, 1997.

VIAL Stéphane, *La structure de la révolution numérique. Philosophie de la technologie*, Thèse de doctorat présentée à l'Université Paris Descartes, soutenue le 21 novembre 2012.

Articles

LELEU-MERVIEL Sylvie, « Les désarrois des 'Maîtres du sens' à l'ère numérique », dans *Créer du sens à l'ère numérique.*H_2PTM_{03}, Hermès, 2003.

MVUEZOLO MIKEMBI Ignace, « Le transfert de la technoscience en Afrique. Problèmes et pistes de réflexion », dans *Identités culturelles*

africaines et nouvelles technologies. Actes de la XVI[è] Semaine Philosophique de Kinshasa, du 10 au 16 décembre, 2000, FCK, 2002.

MVUEZOLO MIKEMBI Ignace, « Les enjeux d'Internet », dans NDUMBA Y'Oole L'Ifefo Georges (dir.), *Sociétés africaines et nouvelles technologies. Enjeux existentiels.* Revue Philosophique de Kinshasa / Faculté de Philosophie, Vol. n°23-24 (janvier – décembre 1999).

MWEZE Dominique, « Les nouvelles technologies de l'information et de communication et leurs concepts opératoires », dans NDUMBA Y'OOLE L'IFEFO Georges (dir.), *Sociétés africaines et nouvelles technologies. Enjeux existentiels,* Revue Philosophique de Kinshasa, Vol. XIII, (janv.-déc.1999) n°23-24, Faculté de Philosophie, FCK.

NKOMBE OLEKO François, « Les retombées actuelles de la mondialisation », dans *Identités culturelles africaines et nouvelles technologies.* Actes de la XVIe Semaine Philosophique de Kinshasa, du 10 au 16 déc. 2000, FCK, 2002.

PILLOU Jean-François et CAILLEREZ Pascal, *Tout sur les systèmes d'information. Grandes, moyennes et petites entreprises,* 2[ème] édition, Paris, Ed. Dunod, 2011.

VAN PARYS Philippe, « Mondialisation et justice internationale », dans Georges NDUMBA Y'Oole L'Ifefo Georges (dir.), *Sociétés africaines et nouvelles technologies. Enjeux existentiels,* Revue Philosophique de Kinshasa, Vol. XIII, (janv.-déc.1999) n°23-24, Faculté de Philosophie, FCK.