Plan

Objectifs du module

Bienvenue dans le module de connaissances d'introduction dans le cadre du projet GFCE-Afrique. Ce module vise à donner aux utilisateurs une meilleure compréhension des concepts clés et des défis sous-jacents dans le domaine de la cybersécurité, ainsi qu'à les inciter à « adhérer » à la cybersécurité, en créant un lien entre la cybersécurité et d'autres questions pertinentes en termes de politique numérique, telles que l'économie et les droits humains.

Le module s'adresse aux non-spécialistes, aux responsables politiques, aux décideurs impliqués dans divers domaines (affaires étrangères, développement économique, sécurité et criminalité, télécommunications, finances, etc.) et à ceux qui souhaitent se familiariser avec le concept de cybersécurité, les risques et acteurs principaux, et le contexte plus large.

À la fin de ce module, vous serez en mesure de répondre et de trouver des ressources supplémentaires pour les questions suivantes :

Cartographie de la cybersécurité

- Qu'est-ce que la cybersécurité, et que recouvre le concept de cybersécurité ?

- Qui sont les principaux auteurs de cyberattaques et quelles sont les principales cibles ?
- Quels sont les principaux risques liés à la cybersécurité sur le continent africain ?

Cybersécurité et économie
- Quelles sont les conséquences de la numérisation rapide sur l'économie en termes de sécurité ?
- Dans quelle mesure le renforcement des cybercapacités peut-il avoir un impact positif sur les services financiers numériques ?

Cybersécurité et droits humains
- Quelle est l'interaction entre les droits humains et la sécurité ?
- Une sécurité accrue implique-t-elle moins de vie privée et de liberté d'expression pour les utilisateurs d'Internet ?
- Comment relever les défis pressants en matière de libertés sur Internet ?

Nous vous recommandons de prêter attention à ce module, même si vous le suivez uniquement dans la perspective des modules à venir. En effet, nous présenterons les choses globalement, en contexte. Bonne chance pour la formation qui vous attend.

1 Introduction : Interdépendance numérique et défis géostratégiques

Le cyberespace est une composante essentielle de la société moderne. Les services gouvernementaux, le secteur financier et les infrastructures sociétales essentielles, notamment les écoles et les hôpitaux, dépendent de plus en plus, et de manière irréversible, de l'interconnectivité et du réseau mondial. Les particuliers dépendent également de l'Internet : le nombre d'internautes dans le monde a dépassé la barre des 5,1 milliards en juin 2021, soit plus de 65 % de la population totale. La pandémie de COVID-19 a encore accéléré la transition vers la vie en ligne, très probablement de manière irréversible, faisant de nos appareils connectés et des services en ligne nos compagnons toujours plus fidèles.

Ce scénario, qui relevait autrefois de la science-fiction, présente de nombreux avantages pour tous, de la simple commodité à l'accès omniprésent à l'information et à la connaissance, comme de l'automatisation des processus à des systèmes hautement efficaces. Ces avantages s'accompagnent de risques de sécurité de plus en plus sophistiqués et importants, allant d'une éventuelle défaillance ou d'attaques contre l'infrastructure Internet (avec l'inaccessibilité des services qui en découle) à des violations de données à caractère personnel, en passant par l'utilisation abusive et la manipulation d'informations, de voitures autonomes piratables ou d'armes létales autonomes.

Ces risques doivent être abordés de manière globale et systématique. Comme nous le verrons dans la suite de ce cours, nombreux sont les pays qui ont adopté des stratégies nationales de cybersécurité et des législations associées (prenant parfois en compte la sécurité comme les libertés). Un nombre croissant de pays ont mis en place des mécanismes nationaux de réponse aux cyberincidents, impliquant le gouvernement ainsi que les secteurs des entreprises, des universités et de la société civile. Certains ont déclaré que le « cyber » constituait le cinquième domaine militaire (après la terre, la mer, l'air et l'espace) et ont mis en place des cybercommandements défensifs et offensifs au sein de leurs forces armées.

La cybersécurité est passée au premier plan de l'agenda diplomatique et politique international au sein des comités des Nations Unies (ONU), de l'Organisation du traité de l'Atlantique Nord (OTAN), de l'Union internationale des télécommunications (UIT), de l'Organisation mondiale du commerce (OMC), du Conseil de l'Europe (CdE), de l'Organisation de coopération et de développement économiques (OCDE), de l'Organisation pour la sécurité et la coopération en Europe (OSCE), du Forum régional de l'ASEAN (ARF), de l'Organisation des États américains (OEA), du Commonwealth, du Groupe des Sept (G7) et du Groupe des Vingt (G20), pour ne citer que quelques-uns des principaux forums. Entre temps, l'attention portée à l'éventualité d'un cyberconflit passe de l'ignorance totale à un battage médiatique excessif, en raison de la méconnaissance générale et de l'orientation sécuritaire souvent étroite des discussions politiques actuelles. Les débats se poursuivent concernant la façon de protéger l'industrie et les infrastructures critiques, de plus en plus (inter)connectées, contre les cyberattaques. La cybercriminalité, qui s'inscrit souvent dans notre réalité vécue, est traitée dans le cadre de différents processus internationaux. Les autorités judiciaires et les services répressifs de nombreux pays coopèrent au-delà des frontières, à un niveau opérationnel, pour lutter contre la cybercriminalité (dans les limites des instruments bilatéraux et multilatéraux actuels).

Les risques sont de plus en plus sophistiqués et les groupes désireux d'exploiter les vulnérabilités du cyberespace sont passés des communautés clandestines de hackers « black hat » à des groupes criminels mondiaux et bien organisés, aux services de sécurité des gouvernements et aux forces de défense nationales. Pour compliquer encore les choses, la plupart des cibles (infrastructures et services Internet) sont privées et les opérateurs sont dispersés dans différentes juridictions mondiales.

La section suivante donne un aperçu plus détaillé du concept de cybersécurité et aborde les principaux risques et défis, notamment dans le contexte de l'Afrique.

2 Cartographie de la cybersécurité

2.1 Présentation du concept

- Qu'est-ce que la cybersécurité, et que recouvre le concept de cybersécurité ?

L'Internet et les politiques publiques numériques sont en constante évolution. Il existe donc une grande confusion terminologique, allant de différences plutôt mineures comme l'utilisation interchangeable de préfixes (cyber/e/digital/net/virtual) à des différences fondamentales, où l'utilisation de différents termes reflète des approches politiques différentes. Le domaine de la cybersécurité présente un fort potentiel de confusion : la base de données mondiale des définitions du cyberespace de 2015 contient plus de 400 définitions politiques de termes liés à la cybersécurité et à la sécurité de l'information !

Plusieurs termes similaires sont utilisés de manière interchangeable lorsqu'il est question de cybersécurité :

- cybersécurité
- sécurité informatique
- sécurité de l'information
- sécurité des systèmes d'information

- sécurité TI
- sécurité des réseaux
- sécurité des données

Cependant, ils n'ont pas exactement la même signification.

Point de réflexion

Comment définiriez-vous chacun de ces termes ? Veuillez proposer vos propres définitions ou partager une définition que vous avez trouvée.

La théorie de la sécurité de l'information nous fournit quelques concepts de base. Si l'on se réfère à la triade CIA (Figure 1), la *confidentialité* interdit la divulgation non autorisée d'informations (p. ex., la lecture des e-mails d'autres personnes), l'*intégrité* interdit la modification non autorisée d'informations (p. ex., la modification des instructions de paiement électronique) et la *disponibilité* garantit que les informations sont réellement disponibles (par exemple, l'accès aux bulletins de vote électronique)[1]. La sécurité de l'information concerne donc principalement la protection des informations (numériques) ; dans la pratique en revanche, la cybersécurité consiste souvent à protéger les appareils, les réseaux et les systèmes qui utilisent des informations (numériques).

Figure 1. La triade CIA de la sécurité de l'information
Source : Burnette, 2020

Les discussions politiques mondiales sont dominées par ces deux termes : cybersécurité et sécurité de l'information. Cependant, l'approche de la cybersécurité peut varier en fonction des différentes parties prenantes. Tandis que les institutions publiques se concentrent sur la sécurité de l'État, les communautés des droits humains suggèrent que la cybersécurité devrait concerner les personnes plutôt que les systèmes. Puddephatt et Kasper définissent ce point comme une question de sécurité individuelle plutôt que de sécurité nationale (observant que des pratiques telles que la surveillance sont diamétralement opposées à la sécurité individuelle). La Coalition pour la liberté en ligne (un partenariat de 30 gouvernements œuvrant à la promotion de la liberté de l'Internet) a codifié une

[1] Mark Stamp, *Information Security: Principles and Practice*. Hoboken, New Jersey : John Wiley & Sons, 2011.

perspective similaire, en définissant la cybersécurité comme la protection de l'information et de l'infrastructure de l'Internet, dans le but d'améliorer la sécurité des individus, tant en ligne que hors ligne.

2.2 Principaux risques, cibles et auteurs de cyberattaques

- Qui sont les principaux auteurs de cyberattaques et quelles sont les principales cibles ?

Les cyberattaques englobent une multitude d'activités criminelles, allant du vol d'un mot de passe personnel ou du piratage d'un système sensible à l'espionnage d'entreprises et de gouvernements, en vue d'acquérir des informations sensibles.

Au début, les auteurs de cyberattaques étaient surtout des « geeks », c'est-à-dire des personnes compétentes en matière de TIC, qui étaient capables de pirater des systèmes, de développer des logiciels malveillants et de mener des cyberattaques. Toutefois, avec le développement des marchés criminels en ligne, les cyberoutils sont facilement accessibles à tout criminel disposant de certaines ressources financières et des compétences minimales pour accéder à ces marchés. Il est souvent difficile d'identifier la personne ou l'entité exacte à l'origine d'une cyberattaque ; en effet, les pirates peuvent utiliser plusieurs appareils ou faire appel à des personnes dispersées à l'échelle du globe pour mener une attaque. Un changement de paradigme dans la cybersécurité a été introduit avec l'entrée des gouvernements (et leurs vastes ressources humaines et financières) et leurs intérêts géopolitiques, dans la liste des auteurs d'attaques. Il ne faut pas oublier non plus que si les acteurs doivent être basés à proximité relative de la cible pour constituer une réelle menace dans l'espace physique, il n'en va pas de même dans le cyberespace : les acteurs peuvent se trouver n'importe où dans le monde, jusqu'à des milliers de kilomètres des cibles, et cette présence incognito renforce le poids du problème. Les menaces prennent généralement la forme d'attaques et des outils nécessaires pour mener ces attaques, dont la portée et la sophistication ne cessent de croître.

Les outils d'attaque les plus courants sont l'utilisation de logiciels malveillants, ainsi que le spam, les escroqueries en ligne et les techniques d'hameçonnage. Les infrastructures critiques et les structures gouvernementales, quant à elles, font souvent l'objet d'une attaque connue sous le nom de menace persistante avancée (APT) : une attaque qui combine différents outils et techniques pour permettre un accès non autorisé au système et un séjour prolongé non détecté à l'intérieur de celui-ci (pouvant s'étendre sur plusieurs années), afin de voler des informations sensibles (à des fins d'espionnage, notamment) ou de saboter le système.

Les logiciels malveillants sont à l'origine de la plupart des attaques qui vont au-delà d'un simple canular ou d'une fraude. Le logiciel malveillant exploite les failles du système d'exploitation de la victime ou de certains des composants logiciels ou matériels utilisés. Certains types de logiciels malveillants très sophistiqués ciblent des systèmes complexes spécifiques de contrôleurs et peuvent entraîner des dommages physiques dans une installation. Enfin, les logiciels malveillants sont une composante fondamentale de l'une des cyberarmes les plus puissantes d'aujourd'hui : les botnets. Ces ordinateurs « zombies » contrôlés à distance (ou bots) sont utilisés pour voler des données personnelles et des identifiants ou pour mener des attaques sur d'autres ordinateurs à l'insu de leurs propriétaires.

Les chevaux de Troie, les virus et les vers sont classés parmi les logiciels malveillants (Figure 2).

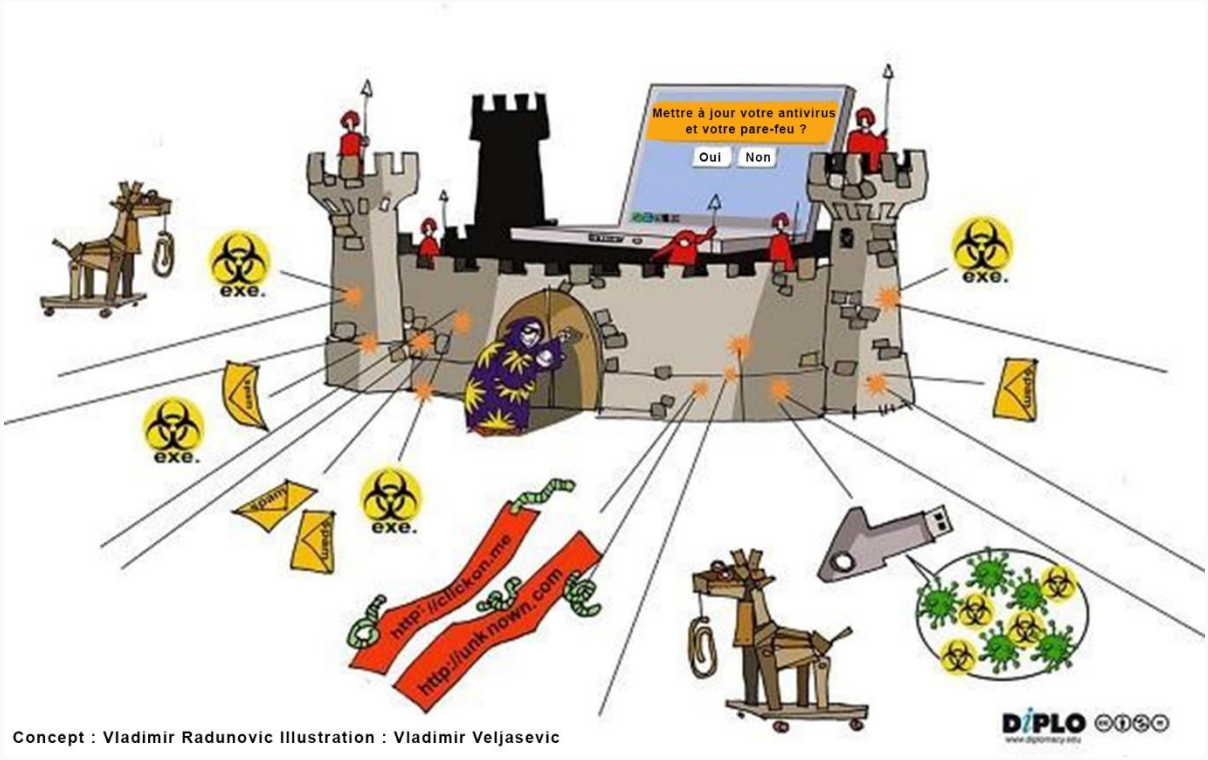


Figure 2. Il est possible d'éviter la plupart des menaces liées aux logiciels malveillants grâce à un logiciel antivirus à jour.

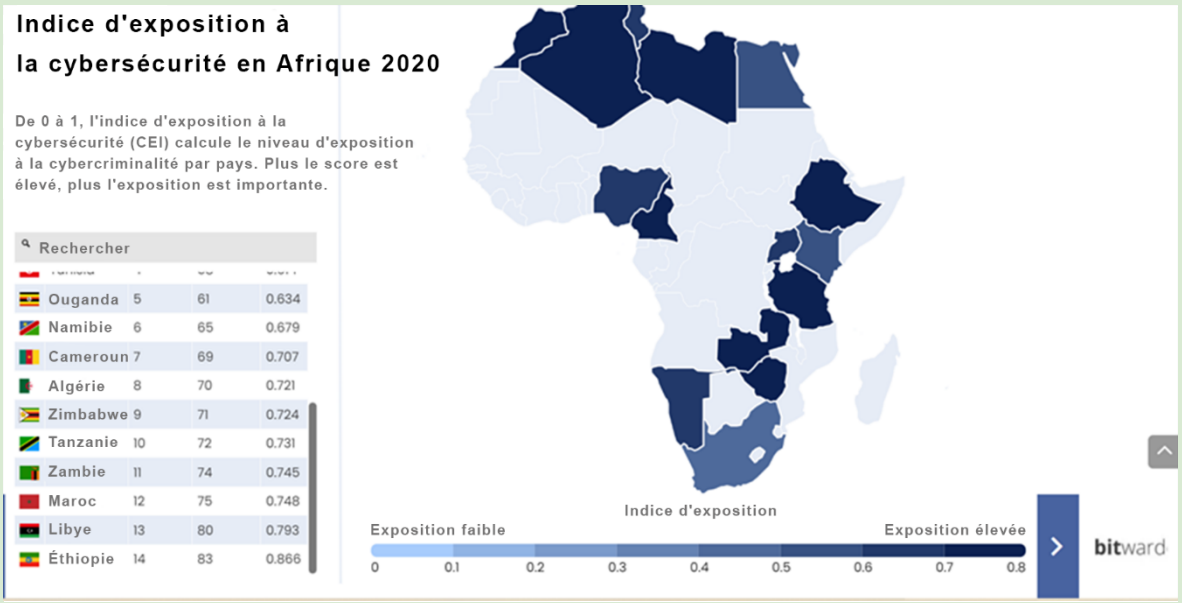
Si, par le passé, les logiciels malveillants étaient réservés aux programmeurs et aux pirates informatiques hautement qualifiés, une grande variété de codes est aujourd'hui facilement disponible sur les marchés noirs en ligne. AV-Test, un institut de sécurité informatique indépendant situé en Allemagne, indique qu'il enregistre chaque jour plus de 450 000 nouveaux programmes malveillants et applications potentiellement indésirables. Les logiciels malveillants se propagent principalement par la diffusion de fichiers infectés apparemment légitimes (fichiers exécutables, fichiers MS Office, voire PDF et photos) joints à un e-mail ou à un message sur les médias sociaux. Ils peuvent également être intégrés sous la forme de scripts malveillants sur de faux sites web (souvent sous la forme d'un « kit d'exploitation », conçu pour identifier les vulnérabilités logicielles des appareils accédant au site web et permettant à l'attaquant d'y implanter à distance son code malveillant), ou même sur des sites web légitimes mais infectés. Si l'intention est de lancer une attaque massive, comme dans le cas d'un ransomware, les botnets de spam sont souvent utilisés pour effectuer la distribution à grande échelle de pièces jointes ou de liens web dans les bases de données compromises d'e-mails, dans l'espoir que les destinataires activent le logiciel malveillant. Les attaques ciblées, en revanche, font appel à des méthodes d'hameçonnage sophistiquées pour garantir que la cible visée activera la pièce jointe ou le lien. Certains virus peuvent se propager via USB et Bluetooth ; Stuxnet est un exemple typique de virus qui a pu infiltrer le système « air-gapped » (non connecté à l'Internet) via des clés USB.

Testez vos connaissances !

Savez-vous ce que signifient les principaux concepts liés aux attaques de cybersécurité ? **Testez vos connaissances ici** et lisez-en davantage, si nécessaire.

Étude de cas : Quels sont les principaux risques liés à la cybersécurité sur le continent africain ?

En matière de pénétration de l'Internet, l'Afrique est le continent qui connaît la croissance la plus rapide. On estime que le pourcentage de personnes utilisant l'Internet est passé d'à peine 2,1 % en 2005 à 43 % en décembre 2020. Si le fossé entre les nantis et les démunis du numérique se réduit lentement, le fossé de la cybersécurité semble se creuser. Selon le dernier rapport sur l'indice mondial de cybersécurité publié par l'UIT, seuls quatre pays d'Afrique subsaharienne (Maurice, Tanzanie, Ghana et Nigeria) figurent parmi les 50 pays ayant les indices de cybersécurité les plus élevés. En outre, les données montrent que l'Afrique est le pays le plus exposé aux cyberattaques. L'image ci-dessous montre le niveau d'exposition à la cybercriminalité par pays.



Les risques liés à la sécurité sont nombreux et variés, et différents acteurs ont identifié les principaux problèmes et menaces qui méritent de retenir l'attention. Par exemple, INTERPOL a recensé les menaces les plus importantes en se fondant sur ses propres informations, sur les contributions de ses pays membres et sur les données fournies par des partenaires du secteur privé. Il s'agit notamment des escroqueries en ligne ; de l'extorsion numérique, dans laquelle les utilisateurs sont amenés par la ruse à partager des images compromettantes qui sont utilisées à des fins de chantage ; de la compromission des e-mails professionnels, dans laquelle les criminels piratent les systèmes de messagerie pour obtenir des informations sur les systèmes de paiement des entreprises, tout en incitant les employés à transférer de l'argent sur leur compte bancaire ; des ransomwares et des botnets.

L'analyse réalisée pour l'ACSS (Africa Center for Security Studies) met en évidence quatre grandes catégories de risques pour la sécurité : l'espionnage, le sabotage des infrastructures critiques, le crime organisé et les contours changeants du champ de bataille africain. Le cyberespionnage (le piratage de systèmes antagonistes pour obtenir des données sensibles) est très répandu, car la numérisation rapide et l'accès croissant aux nouvelles technologies permettent à un large éventail d'acteurs de mener de telles activités. Les attaques contre les systèmes critiques deviennent également plus fréquentes, visant le plus souvent les banques. On constate également une augmentation des cyberattaques ciblant les infrastructures maritimes. Le troisième risque fait référence à la fois aux fraudes et aux vols en ligne, comme la compromission des e-mails d'affaires, mais aussi à un crime organisé traditionnel qui se déplace vers l'environnement en ligne. La dernière catégorie fait référence à l'intégration des technologies émergentes, telles que les drones et les systèmes d'IA, dans le combat moderne, avec des implications significatives pour les opérations militaires et les tactiques du champ de bataille.

Contribuer et s'engager

Le module 3a se concentre sur la cybercriminalité, son impact et les réponses apportées par les forces de l'ordre. Reportez-vous au module dédié pour plus d'informations sur le sujet.

Inscrivez-vous au cours en ligne sur la cybersécurité de Diplo ! Ce cours avancé en ligne de 10 semaines sur la cybersécurité couvre les risques technologiques et géopolitiques, les défis politiques, les acteurs et les initiatives liés à la cybersécurité, en particulier ceux liés à la cybercriminalité, à la violence, à la protection de l'enfance, à la sécurité des infrastructures essentielles et à la cyberguerre. Il couvre également un contexte plus large : les relations de la cybersécurité avec le développement économique et les droits humains.

3 Le contexte plus large de la cybersécurité

La cybersécurité ne peut être examinée sans tenir compte d'un contexte plus large et de ses liens avec d'autres défis liés à l'Internet et à la gouvernance. La figure 3 montre dans quelle mesure la cybersécurité est liée à d'autres domaines importants de la politique numérique et de la gouvernance de l'Internet, tels que les droits humains et l'économie. Cette section explorera donc l'interaction entre la cybersécurité et les domaines de politique numérique susmentionnés, et abordera les principaux défis propres au continent africain.

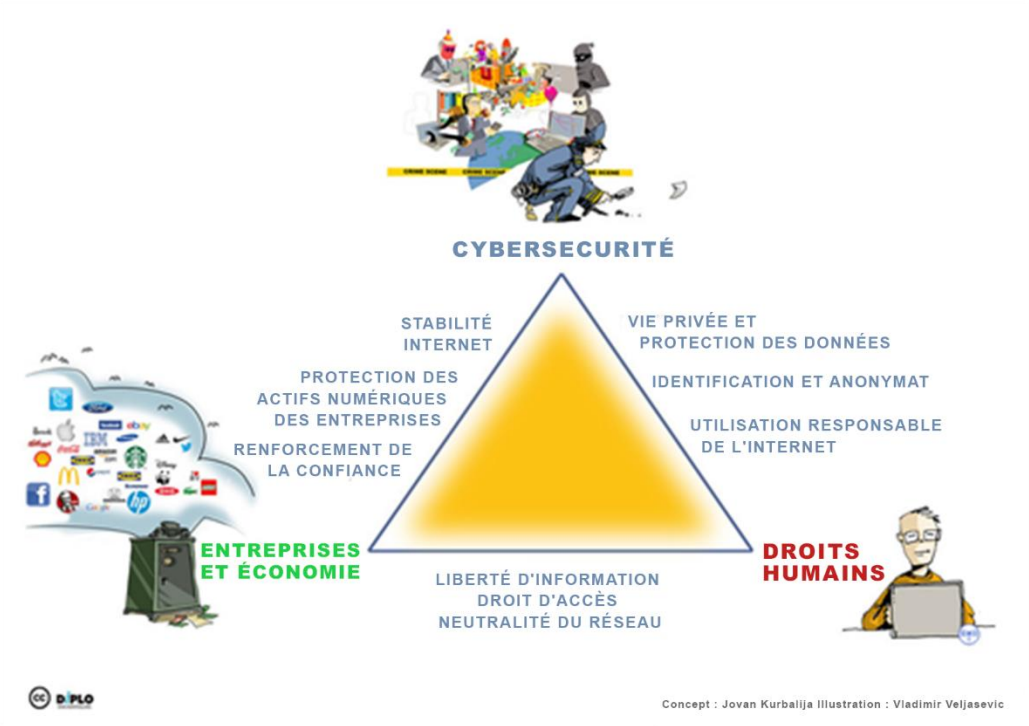


Figure 3. Un triangle de perspectives pour les politiques numériques : cybersécurité, droits humains, et développement économique et commercial. Source : DiploFoundation.

3.1 Cybersécurité et économie : le renforcement des cybercapacités comme moyen d'inspirer la confiance dans l'économie numérique

Dans la section d'introduction de ce module, nous avons vu comment un environnement en ligne stable et sécurisé contribue à la paix et à la sécurité internationales, ainsi qu'à la confiance entre les acteurs du cyberespace. La confiance est une condition préalable à l'essor de l'économie numérique, et ce point est particulièrement vrai pour les transactions de commerce électronique.

La vente de produits et de services sur l'Internet se fait sans contact physique ; en conséquence, les consommateurs s'inquiètent de différents aspects de la transaction, tels que la légitimité du vendeur, la qualité du produit, la possibilité que leurs données personnelles soient utilisées à mauvais escient (par le vendeur ou par un tiers), et les menaces potentielles posées par des acteurs malveillants et des criminels en ligne. Selon le rapport conjoint de la CNUCED, du CIGI et d'IPSOS sur l'état de l'économie numérique mondiale, les consommateurs renoncent à acheter des biens ou des services en ligne principalement en raison d'un manque de confiance, comme le montre la figure 4.

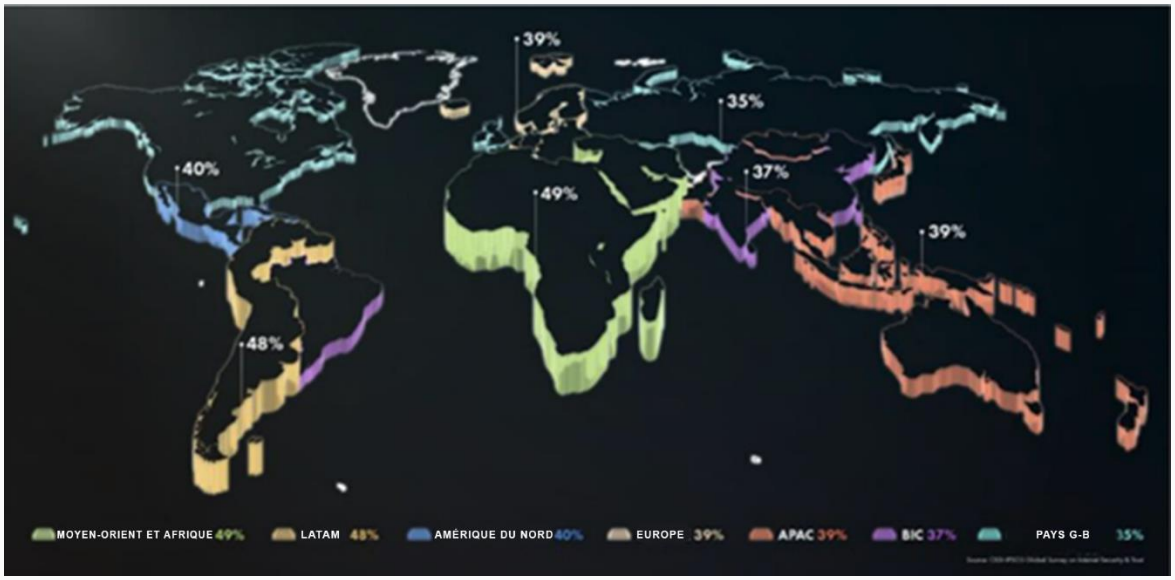


Figure 4. Pourcentage de consommateurs qui mentionnent le manque de confiance comme raison principale pour renoncer aux achats en ligne de biens ou de services. Source : Chung and Yu, 2021

L'édition 2019 du rapport du CIGI et d'IPSOS a confirmé cette tendance, et a souligné que les cybercriminels constituent le facteur principal ayant contribué à accroître le niveau d'inquiétude des consommateurs, suivi par la possibilité d'une utilisation abusive des informations personnelles de la part des sociétés Internet, comme le montre la figure 5.

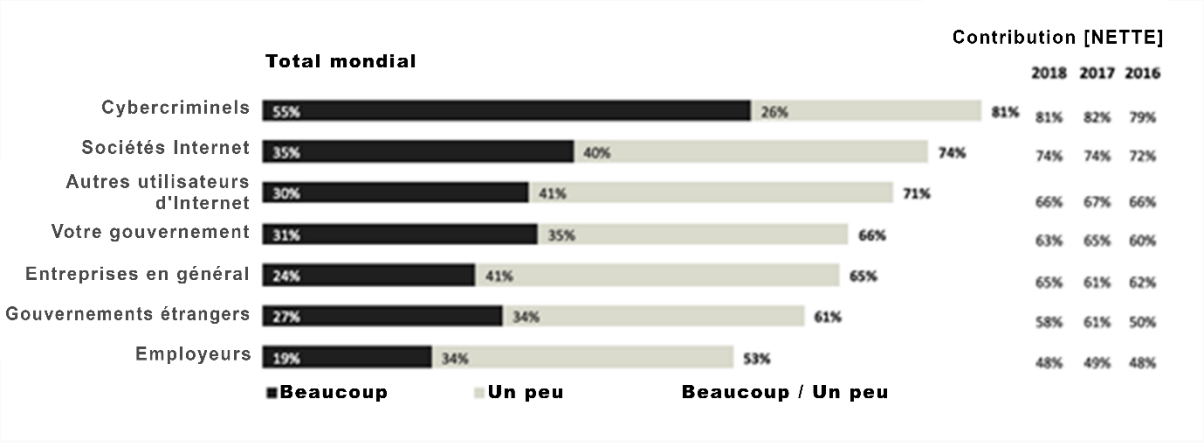


Figure 5. Sources d'inquiétude concernant la protection des informations personnelles. Source : IPSOS, 2019.

Point de réflexion

Existe-t-il des exemples d'enquêtes similaires visant à évaluer la confiance en ligne, menées dans votre pays ou votre région ? Les préoccupations liées à la sécurité des internautes et de leurs données ont-elles un impact négatif sur la croissance des entreprises en ligne et du commerce électronique ? Quelles pourraient être les conséquences économiques si ces préoccupations ne sont pas prises en compte ?

Laissez votre commentaire ci-dessous.

3.1.1 Numérisation de l'économie et sécurité

- Quelles sont les conséquences de la numérisation rapide sur l'économie en termes de sécurité ?

Depuis le déclenchement de la pandémie de COVID-19, l'utilisation d'Internet n'est plus un choix, mais une nécessité. Nous nous appuyons de plus en plus sur l'Internet pour travailler, étudier, accéder aux soins de santé, communiquer et acquérir des produits et des services. Le commerce électronique est désormais essentiel pour l'achat des produits de première nécessité et concerne de plus en plus la plupart des particuliers. La pandémie a entraîné un changement durable des habitudes d'achat à l'échelle du globe, accélérant l'adoption du commerce électronique d'environ cinq ans.

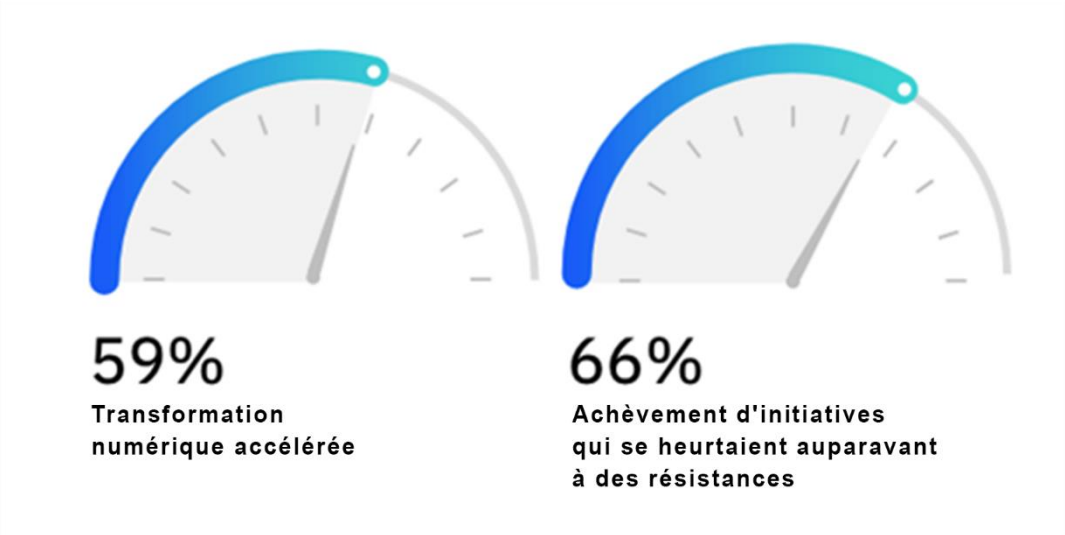


Figure 6. Le sentiment d'urgence autour de la transformation numérique créé par la pandémie de COVID-19. Source : IBM, 2020

Ce scénario de numérisation rapide signifie qu'un plus grand nombre d'entreprises et de particuliers seront confrontés à la commodité, mais aussi aux défis, liés aux opérations dans un environnement en ligne.

La cybercriminalité est l'un des principaux risques en matière de cybersécurité, avec des effets profonds sur le commerce numérique. On a estimé qu'en 2017, le coût de la cybercriminalité pour le continent africain s'est monté à 3,5 milliards de dollars américains. Les estimations portant sur les coûts annuels de la cybercriminalité pour l'économie mondiale varient considérablement. Selon l'Online Trust Alliance (OTA) de l'Internet Society, l'impact économique mondial de la cybercriminalité représentait au moins 45 milliards de dollars US en 2018, tandis qu'un rapport de la société de sécurité McAfee et du Center for Strategic and International Studies (CSIS) a estimé que la cybercriminalité a coûté jusqu'à 600 milliards de dollars US en 2017 à l'économie mondiale. Qu'est-ce que

Le consensus est que le coût de la cybercriminalité suit une tendance haussière, comme le montre la figure 7.

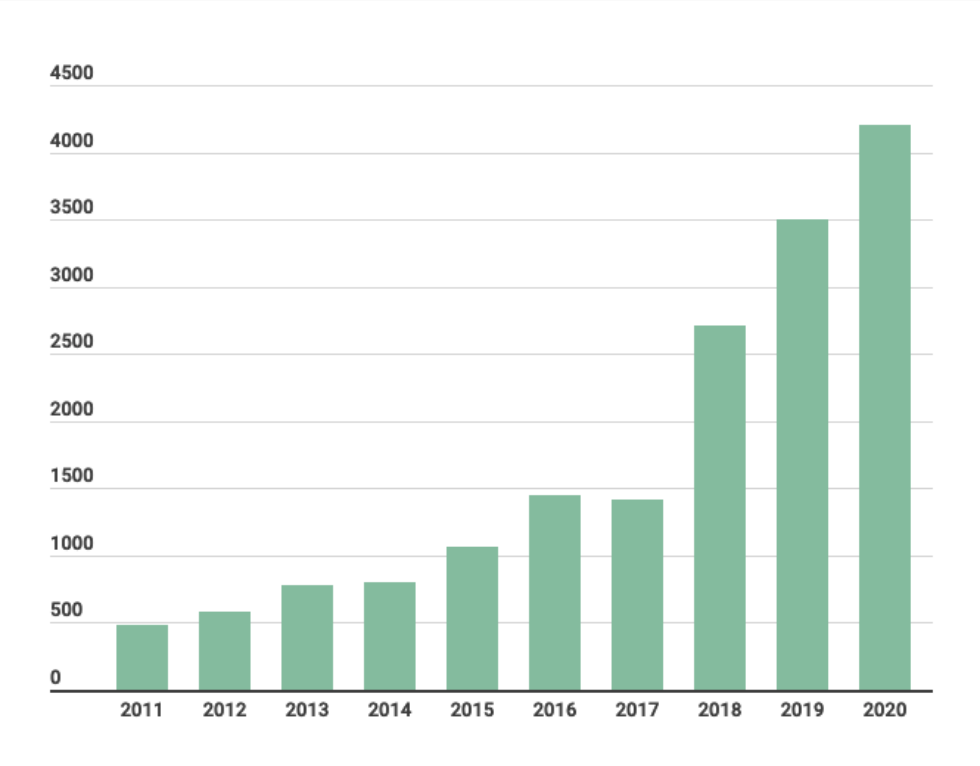


Figure 7. Pertes économiques annuelles dues à la cybercriminalité (en millions de dollars). Source : Diplo, adapté de FBI, 2020

Contribuer et s'engager

Le module 3a se concentre sur la cybercriminalité, son impact et les réponses apportées par les forces de l'ordre. Reportez-vous au module dédié pour plus d'informations sur le sujet.

Outre les pertes financières subies du fait de la cybercriminalité, il existe d'autres effets négatifs pour l'économie :

- **Diminution de la confiance des consommateurs :** lorsque les consommateurs ont été victimes de la cybercriminalité, sans aucune forme de réparation, ils choisissent généralement de ne plus acheter de biens et de services en ligne, et cette attitude se ressent sur les bénéfices des entreprises. On constate dans le monde entier de plus en plus d'attaques réussies menées sur les serveurs des entreprises afin de dérober les données personnelles des clients. En septembre 2021, plus d'un million de citoyens sud-africains ont vu leurs données personnelles exposées (en particulier le nom et les coordonnées des clients, les informations relatives à l'emploi et au salaire, et les informations relatives aux dettes) à la suite d'une attaque menée contre une

entreprise de services de recouvrement de dettes. Ces incidents sapent la confiance des utilisateurs dans les services en ligne.

- **Perte de secrets commerciaux :** la propriété intellectuelle, comme les secrets commerciaux, est une ressource de plus en plus importante pour la plupart des industries. Lorsque ces secrets commerciaux sont volés par suite d'un acte de cybercriminalité, la valeur de leurs actifs diminue.
- **Refus d'accès à certains marchés :** nombreux sont les commerçants qui refusent d'effectuer des transactions de commerce électronique, ou même de conclure de nouveaux services dans certains pays. Le Nigeria se range parmi ces pays en raison des nombreux cas d'activités frauduleuses qui y seraient perpétrées.
- Dans certains cas, des **menaces pèsent sur les infrastructures critiques**, les systèmes financiers et bancaires, et la sécurité nationale.

Le passage au télétravail et aux achats en ligne lié à la pandémie de COVID-19 exige de se concentrer davantage sur la cybersécurité, en raison de la plus grande exposition au cyberrisque. Le commerce électronique a également été touché par la pandémie de COVID-19 ; en effet, la vente de produits de contrefaçon et de services en ligne malveillants présentés, par exemple, comme des applications de dépistage des contacts, a également explosé. Par exemple, les cybercriminels à l'origine de Ginp, un cheval de Troie bancaire, ont utilisé une application appelée *Coronavirus Finder*. Cette application prétendait fournir des informations sur les personnes infectées par la COVID-19 dans le voisinage de l'utilisateur. L'utilisateur était incité à fournir les détails de sa carte bancaire sous prétexte de payer une taxe de 0,75 € qui lui permettrait de visualiser l'emplacement exact des personnes infectées.

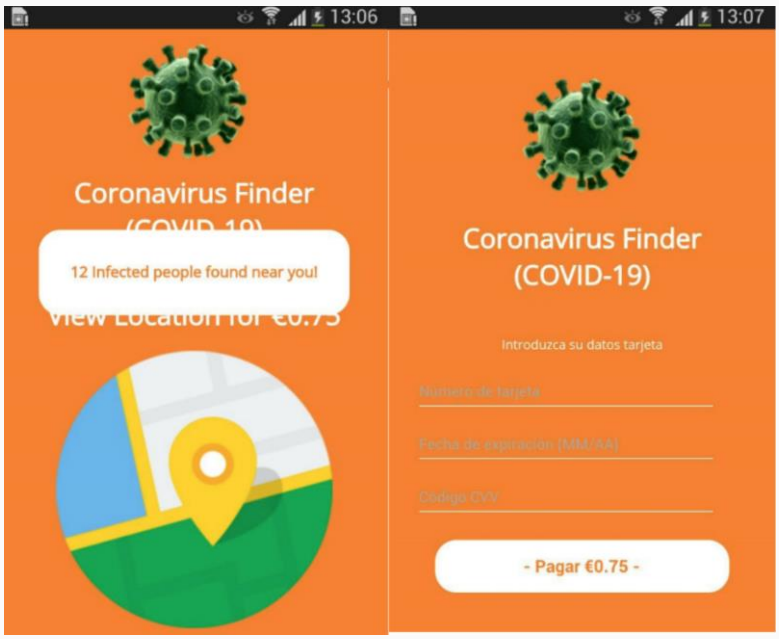


Figure 8. L'application malveillante Coronavirus Finder. Source : Chebyshev, 2020.

Point de réflexion

Comment la pandémie a-t-elle affecté la sécurité des transactions de commerce électronique dans votre pays ou région ? Quel était le type d'incident de sécurité le plus courant (vente de produits de contrefaçon, diffusion de logiciels malveillants, hameçonnage) ? Des mesures concrètes ont-elles été prises pour résoudre ces problèmes ? Lesquelles ?

Laissez votre commentaire ci-dessous.

3.1.2 Services financiers

- Dans quelle mesure le renforcement des cybercapacités peut-il avoir un impact positif sur les services financiers numériques ?

L'économie mondiale repose en grande partie sur le bon fonctionnement des infrastructures financières et essentielles (telles que les télécommunications, l'énergie et les transports) et de la logistique à travers le monde. Ces infrastructures sont exploitées par les secteurs public et privé, et sont considérées comme des points de vulnérabilité importants. Dans le cas des systèmes financiers et bancaires, la transformation numérique rapide brouille les frontières entre les banques et les entreprises technologiques, ce qui rend moins claires les responsabilités en matière de protection de l'infrastructure financière numérique. Selon le Conseil de stabilité financière, « un cyberincident majeur, s'il n'est pas correctement maîtrisé, pourrait perturber gravement les systèmes financiers, y compris les infrastructures financières essentielles, ce qui aurait des répercussions plus larges sur la stabilité financière ».

Dans ce contexte, la sécurité du système financier dépend du développement de la capacité de cybersécurité du secteur financier et de l'investissement dans le renforcement des compétences de la main-d'œuvre en matière de cybersécurité. Le rapport de la Fondation Carnegie pour la paix internationale intitulé « International Strategy to Better Protect the Global Financial System against Cyber Threats » (Stratégie internationale pour mieux protéger le système financier mondial contre les cybermenaces) suggère, entre autres, de créer un mécanisme international pour renforcer les capacités du secteur financier en matière de cybersécurité et d'inclure le renforcement des capacités en matière de cybersécurité dans les programmes d'aide au développement. La Banque africaine de développement a également souligné la nécessité d'intégrer les stratégies de formation et de développement des compétences dans les plans nationaux de développement économique des pays africains.

Les systèmes bancaires et financiers connaissent également une transformation numérique rapide. La combinaison de services financiers et numériques a stimulé l'accès financier à des millions de personnes qui n'étaient pas bancarisées auparavant, comme le montre la figure 9. Les services financiers numériques (SFN) sont essentiels pour la réduction de la pauvreté et la croissance économique. Dans le même temps, les SFN ont accru la complexité liée à la promotion de la sécurité. La fourniture de SFN implique un écosystème complexe, avec la participation d'un groupe d'acteurs divers, tels que les banques, les opérateurs de réseaux mobiles, les fournisseurs et développeurs de plateformes SFN, les agents de détail, les régulateurs, les fournisseurs de services de paiement et les clients. La croissance et l'adoption rapides des SFN et l'interconnexion du système le rendent vulnérable, puisque la sécurité dépend non seulement des mesures adoptées par les fournisseurs eux-mêmes, mais aussi des fournisseurs tiers et des consommateurs.

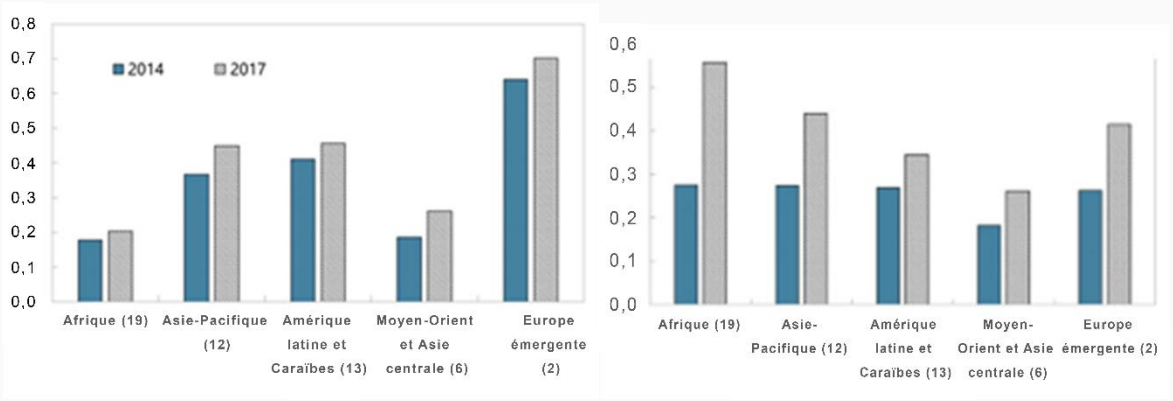


Figure 9. Comparaison entre l'inclusion financière traditionnelle (à gauche) et l'inclusion financière numérique (à droite). Source : Khera, 2021

Les violations de données sont courantes et peuvent diminuer la confiance des clients dans les plateformes de finance numérique. Une plus grande sensibilisation des régulateurs aux cyberrisques a conduit à revisiter le compromis entre efficacité et sécurité dans les services financiers. Dans ce contexte, le « Cadre de garantie de la sécurité des services financiers numériques », élaboré sous la direction de l'UIT, est une ressource pertinente, car il donne une vue d'ensemble des menaces et des vulnérabilités, en matière de sécurité, auxquelles les fournisseurs de services financiers numériques sont confrontés, contribue à clarifier les rôles et les responsabilités, élabore une méthode d'évaluation des risques et formule des recommandations.

De nombreux pays d'Afrique connaissent une mutation radicale de leur secteur financier, à mesure qu'ils étendent l'inclusion financière et passent aux services de paiement direct. On observe une augmentation sans précédent du nombre de personnes bénéficiant d'un accès aux services financiers formels sur le continent, qui abrite désormais plus de déploiements de services financiers numériques que toute autre région du monde, avec près de la moitié des quelque 700 millions d'utilisateurs individuels dans le monde.

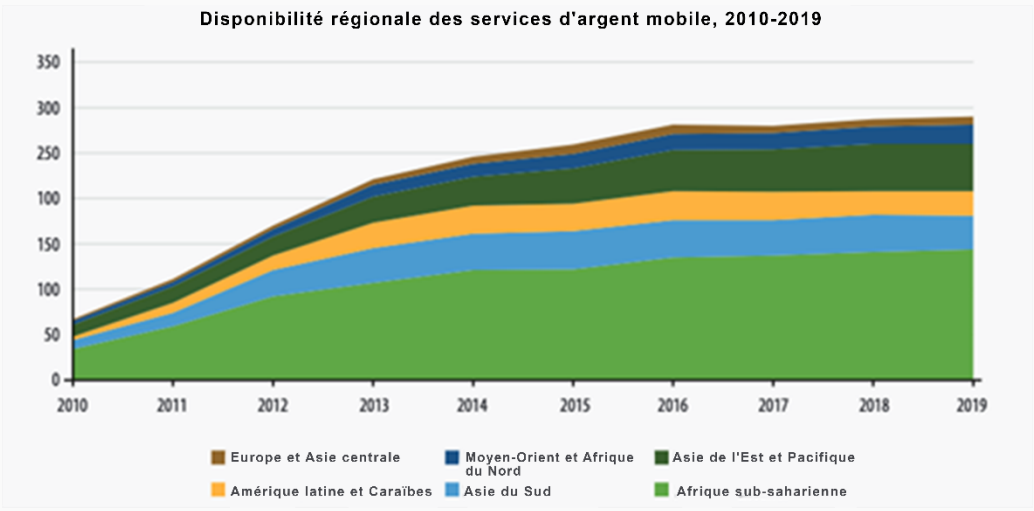


Figure 10. Disponibilité régionale des services d'argent mobile. Source : Nafula Machasio (2020)

La pandémie de COVID-19 a encore accéléré le passage à la finance numérique dans de nombreuses économies. En Afrique, les gouvernements ont promulgué des réglementations en vue de soutenir l'adoption de services financiers numériques, utilisé les SFN pour permettre la mise en place de programmes de transfert de fonds d'urgence, et encouragé l'utilisation de modes de paiement sans espèces et sans contact pour réduire le risque de propagation du virus, tandis que les clients utilisaient de plus en plus le téléphone pour payer les commerçants.

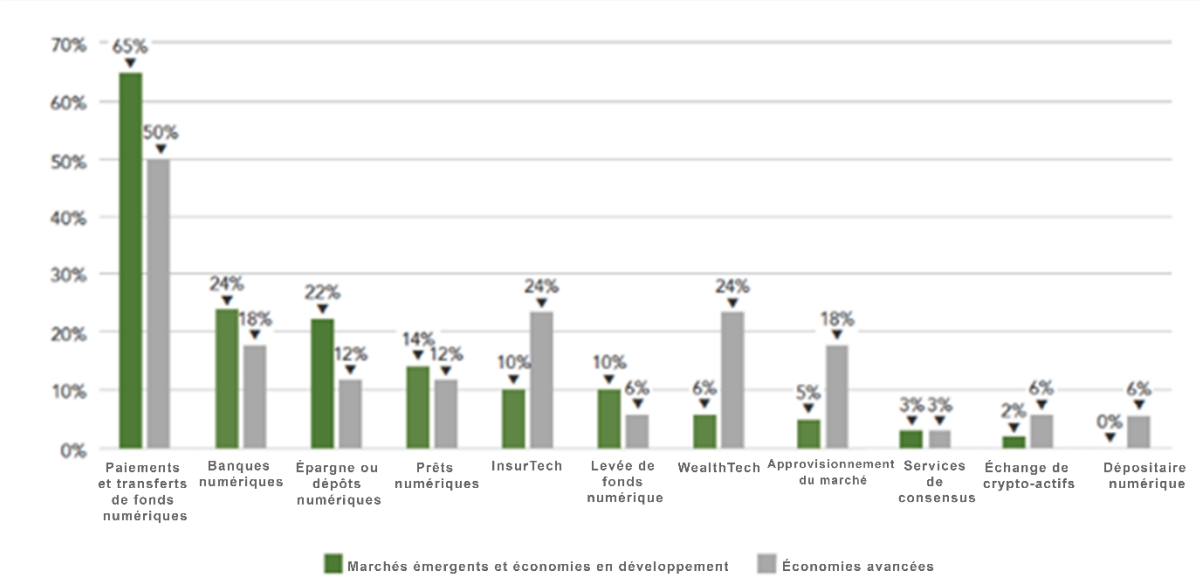


Figure 11. Pourcentage de régulateurs ayant signalé une augmentation de l'utilisation ou de l'offre de fintech compte tenu de la COVID-19 dans les économies émergentes et avancées. Source : Klapper and Miller, 2021.

Le contexte crée des opportunités supplémentaires pour l'adoption des SFN en Afrique. Maurer et Nelson recommandent de renforcer les liens entre l'inclusion financière et la cybersécurité, afin d'améliorer la durabilité des récents progrès réalisés en matière d'inclusion financière sur le continent. Ils suggèrent la création d'un réseau d'experts spécifiquement axé sur la cybersécurité en Afrique.

L'Alliance pour l'inclusion financière (AFI), réseau de plus de 90 pays en développement dans lesquels résident la majorité des personnes non bancarisées dans le monde, est un exemple de plateforme de formation par les pairs, qui a favorisé le dialogue entre les régulateurs africains et le secteur privé, et a permis de renforcer les capacités pour faire progresser l'innovation financière numérique. Entre 2016 et 2018, plus de 160 politiques et réglementations d'inclusion financière ont été mises en œuvre par les décideurs africains grâce à leur engagement dans l'AFI. Le sous-groupe de l'AFI sur la cybersécurité a produit le document « Cybersecurity and financial inclusion: framework & risk guide » (Cybersécurité et inclusion financière : cadre et guide des risques) afin de proposer des principes clés et de bonnes pratiques pour aider les autorités de réglementation et de supervision à concevoir les outils qui permettront au secteur financier de gérer les risques de cybersécurité.

3.2 Cybersécurité et droits humains : les deux sont-ils compatibles ?

- Quelle est l'interaction entre les droits humains et la sécurité ?
- Une sécurité accrue implique-t-elle moins de vie privée et de liberté d'expression pour les utilisateurs d'Internet ?
- Comment relever les défis pressants en matière de droits de l'Internet ?

La cybersécurité est généralement abordée dans le contexte des systèmes nationaux ou internationaux, plutôt que comme un droit de l'individu. Dans le contexte des systèmes nationaux ou internationaux, la discussion sur les droits humains et la sécurité repose souvent une logique binaire : nous pouvons avoir soit les droits humains, soit la sécurité. Toutefois, nous pouvons nous demander s'il est possible d'équilibrer les deux.

Le domaine des droits humains en ligne comprend de nombreuses questions, comme la protection de la vie privée et des données, et la liberté d'expression, pour n'en citer que quelques-unes. Il peut sembler que nous devions évaluer ces droits par rapport à des mesures de sécurité, telles que la surveillance ou le contrôle du chiffrement ; pourtant, certaines mesures peuvent renforcer à la fois la sécurité et les droits, dont l'alphabétisation numérique, l'utilisation intelligente et l'hygiène numérique, comme l'illustre la figure 12.

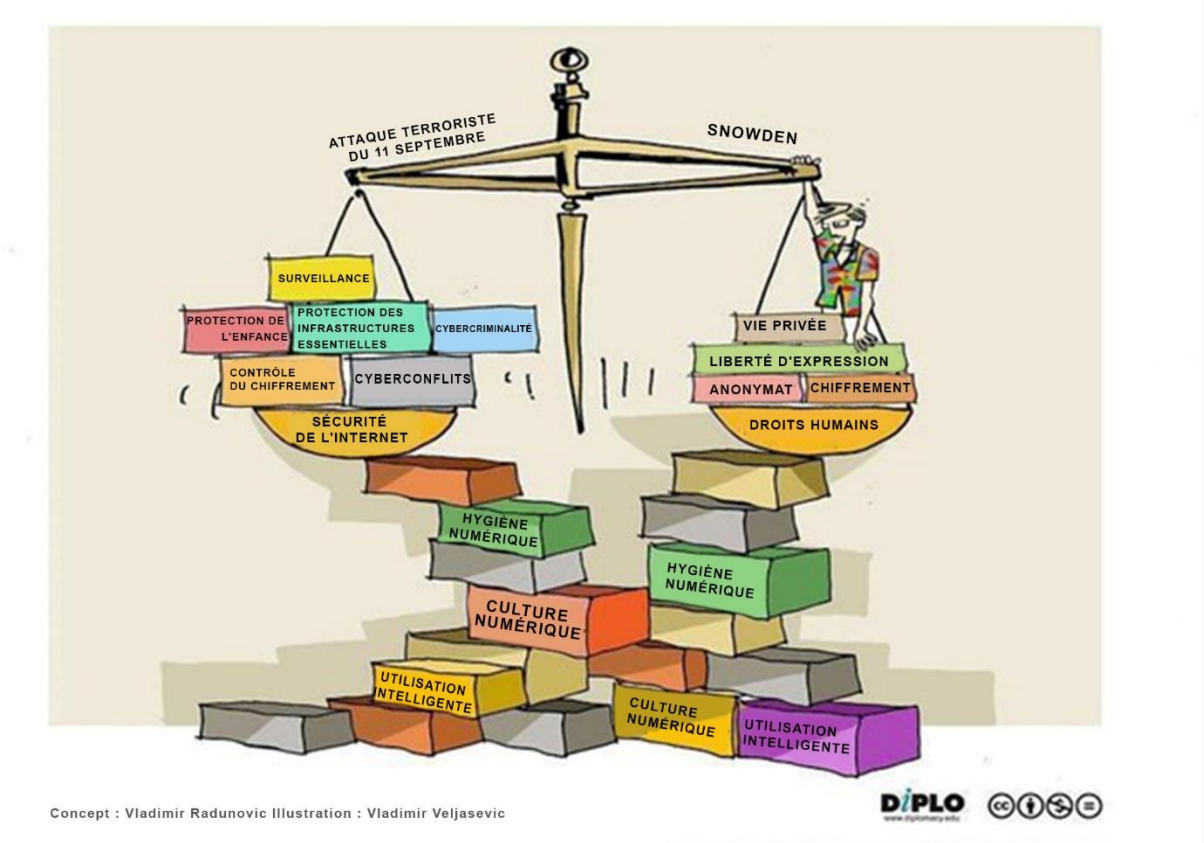


Figure 12. Certaines mesures favorisent à la fois la sécurité et les droits humains

La culture numérique va au-delà des compétences en matière de TIC et implique une évaluation critique de l'impact des technologies numériques sur le développement personnel et la société. Outre les compétences en matière de TIC, elle intègre les trois piliers suivants : l'utilisation intelligente, la promotion de valeurs et la compréhension de l'ère numérique (voir l'illustration ci-dessous). Dans ce contexte, l'utilisation intelligente désigne les compétences nécessaires pour une utilisation responsable et sûre de l'Internet, la promotion des valeurs

implique la pensée critique ainsi que les droits et responsabilités personnels dans le contexte numérique, tandis que la compréhension concerne les implications des concepts sociétaux et économiques de l'ère numérique (par exemple, comment les technologies émergentes changent le marché du travail).

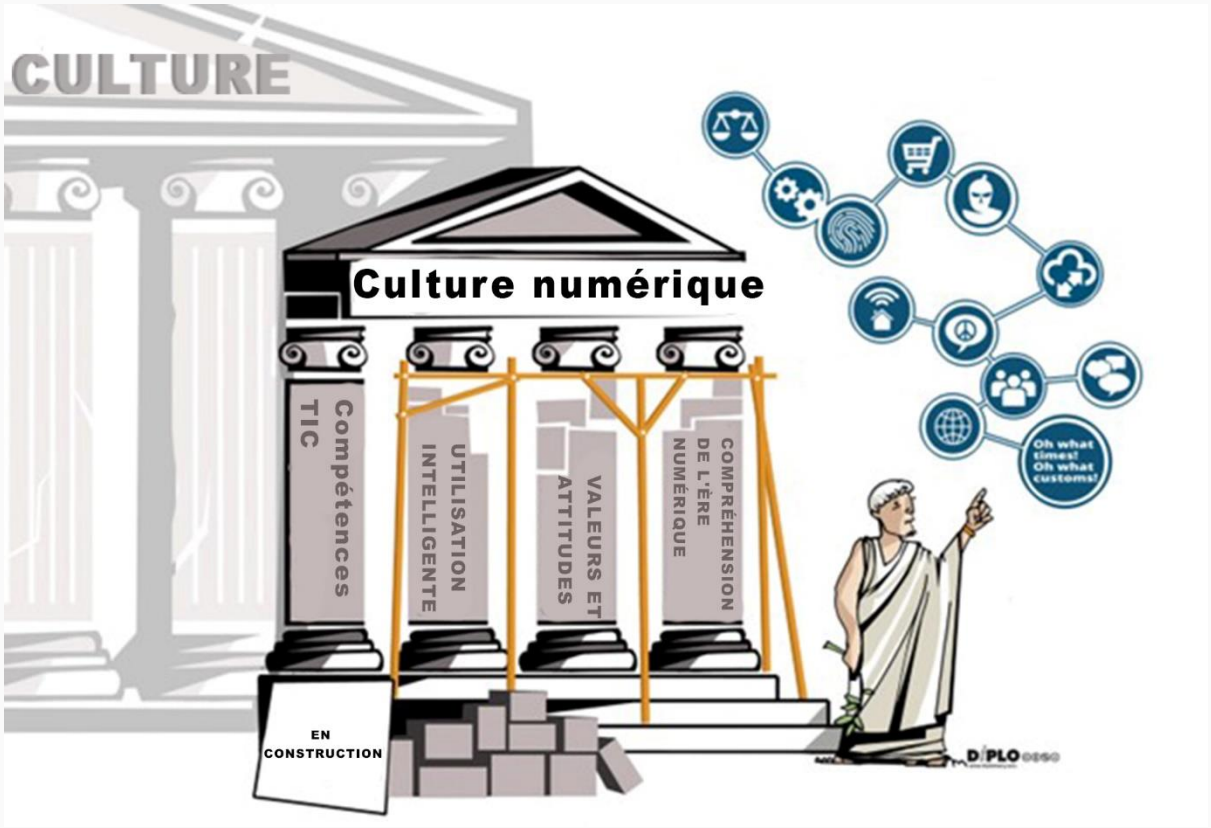


Figure 13. Piliers de la culture numérique
Source : DiploFoundation

Contribuer et s'engager

Pour en savoir davantage sur le renforcement des cybercapacités, l'apprentissage et le développement des compétences, reportez-vous au module de connaissances 4.

Étude de cas : Lois sur la cybersécurité et la cybercriminalité dans la région de la SADC : Implications sur les droits humains

Le rapport publié par MISA Zimbabwe, en partenariat avec la Fondation Konrad Adenauer, examine les lois adoptées et proposées en matière de cybersécurité et de cybercriminalité dans la région de la SADC et leurs implications sur le droit à la vie privée, la liberté d'expression et la liberté des médias. La publication fait également une analyse comparative de ces lois et des conventions, standards et normes internationales.

3.2.1 Vie privée et sécurité

La vie privée et la sécurité en ligne n'ont pas fait l'objet d'un débat international sérieux avant la commercialisation de l'Internet. Cependant, face à l'évolution de l'Internet et de ses composants structurels, les perceptions de ces concepts ont également changé. Dans le passé, la vie privée était principalement abordée dans le cadre de la protection des données personnelles contre la divulgation et le commerce par, et vers, des tiers, tels que Facebook, Google et les agences de publicité. Les attentats terroristes perpétrés aux États-Unis, au Royaume-Uni, en France et en Belgique (entre autres) ont contribué à faire évoluer le discours vers la protection des données personnelles contre leur (mauvaise) utilisation par les gouvernements au nom de la sécurité nationale.

En tentant de définir la vie privée dans les lois nationales, les gouvernements ont mis l'accent sur le traitement des données personnelles et, par conséquent, sur les principes utilisés pour protéger ces informations. Cependant, la définition même des données personnelles varie d'un pays à l'autre. Par exemple, on débat de savoir si une adresse IP, qui fournit une trace indispensable (parfois appelée empreinte électronique) pour la médecine légale en ligne et des informations pour les mesures de protection de la cybersécurité, doit être considérée comme une donnée personnelle, car elle peut, dans certaines circonstances, fournir un lien avec l'identité réelle de la personne qui l'utilise. Le RGPD, par exemple, indique clairement que les « identifiants en ligne », tels que les adresses IP, peuvent être considérés comme des données à caractère personnel. En outre, la Cour de justice de l'UE a statué que même les adresses IP dynamiques peuvent constituer des données à caractère personnel.

Les bases de données gouvernementales contiennent un volume croissant d'informations sur les citoyens. En outre, les politiques de sécurité exigent dans certains cas que le secteur des entreprises (y compris le secteur de l'Internet, qui détient d'énormes quantités de données personnelles sur les clients en ligne) partage ces données avec les services de sécurité et les organismes chargés de faire respecter la loi. La loi britannique sur la surveillance, surnommée « la charte du fouineur » par certains défenseurs des droits humains sur Internet, exige même des fournisseurs d'accès à Internet (FAI) qu'ils conservent les historiques de navigation des utilisateurs pendant un an et les mettent à disposition sur demande des tribunaux, et que les entreprises déchiffrent sur demande les données des utilisateurs. Elle permet également aux services de sécurité de pirater les ordinateurs et les appareils des utilisateurs, bien que les journalistes et certaines autres entités restent à l'abri de cette surveillance. Les groupes de défense des libertés civiles plaident pour la mise en place de mécanismes robustes aux niveaux national et mondial, afin de garantir la protection des données personnelles et d'empêcher leur utilisation abusive par les services de sécurité et les forces de l'ordre.

Il existe cependant une dimension plus directe de la cybersécurité liée aux données personnelles. La multiplication des liens entre les agences gouvernementales et les bases de données du secteur des entreprises, qui contiennent des données personnelles, accroît le risque que les criminels puissent accéder à ces bases de données, qui représentent une ressource très lucrative pour eux. Par conséquent, les gouvernements se voient de plus en plus contraints de créer des réglementations nationales pour la protection des données, non seulement en raison de leurs obligations (et des pressions) de respecter les droits humains, mais aussi en réponse à la nécessité de sécuriser davantage leurs propres services et systèmes.

À l'ère du numérique, le flux de données personnelles et, dans une certaine mesure, le traitement de ces données, sont inévitables. C'est pourquoi les débats politiques actuels

tournent autour de la question de savoir quelles informations sont considérées comme privées, qui devrait pouvoir les collecter et les diffuser, quand et de quelle manière, quelle est la durée acceptable de conservation des données et, enfin, quelles devraient être les normes minimales de traitement et de gestion des données pour garantir la sécurité.

L'UE, par exemple, a adopté en 2006 la directive sur la conservation des données (directive 2006/24/CE), qui oblige les fournisseurs de services de télécommunications et les opérateurs à conserver certaines catégories de données personnelles pendant une période allant de six mois à deux ans. Cette exigence a été fortement contestée par les défenseurs de la vie privée. La directive a été invalidée par la Cour de justice de l'Union européenne en 2014. Le RGPD fournit un cadre complet pour les pays de l'UE et définit également les relations avec les entités situées dans des pays tiers, qui traitent des données personnelles de l'UE. En outre, il définit la responsabilité, exige la « prise en compte du respect de la vie privée dès la conception », définit les notifications de violation de données et réglemente les transferts internationaux, entre autres.

Un autre aspect du débat sur la vie privée et la cybersécurité est lié à l'essor et à l'expansion rapide des médias sociaux et du contenu généré par les utilisateurs. Pour accéder aux sites de médias sociaux ou en devenir membre, les utilisateurs doivent fournir des informations personnelles. En substance, l'utilisateur « paie » les services en ligne en fournissant des données personnelles ; les données sont devenues la monnaie ultime sur l'Internet. Pour aggraver les choses, chaque information téléchargée est généralement copiée plusieurs fois et consignée par des serveurs cache dans le monde entier ; il devient donc difficile, voire impossible, de retirer des éléments de nous-mêmes de l'Internet.

Point de réflexion

Présentation des raisons expliquant la protection limitée de la vie privée en Afrique

Les auteurs de l'article intitulé « Privacy and Security Concerns Associated with Mobile Money Applications in Africa » (Préoccupations en matière de vie privée et de sécurité associées aux applications d'argent mobile en Afrique) visent à élucider les raisons expliquant la faible protection de la vie privée sur le continent africain. Voici un extrait de l'article.

Différentes raisons expliquent les limites de la protection de la vie privée en Afrique. Premièrement, l'Afrique se caractérise en grande partie par une forte tendance communautaire. Cet état d'esprit dévalorise les droits des individus au profit de ceux de la communauté. Dans un tel contexte, la vie privée des individus n'est que peu prise en compte. Deuxièmement, les économies traditionnelles dans lesquelles la communication et le commerce électroniques sont limités ont moins besoin de protéger la vie privée des individus, car il existe peu de moyens de collecter, d'utiliser et d'exploiter les informations sensibles. Jusqu'à très récemment, la grande majorité des Africains ne s'engageait pas dans des opérations de compilation de données. Pour les deux raisons susmentionnées, il n'existe que peu de protections juridiques établies dans les nations africaines.

Que pensez-vous des tentatives susmentionnées d'élucider les raisons expliquant la protection limitée de la vie privée en Afrique ? Sont-elles toujours valables étant donné que l'article a été publié il y a près de dix ans ?

Existe-t-il d'autres raisons spécifiques au continent africain ?

Étude de cas : La protection de la vie privée et des données personnelles en Afrique : une étude basée sur les droits portant sur la législation de huit pays

S'inscrivant dans le cadre d'un projet de la Coalition de la Déclaration africaine des droits et libertés de l'Internet (AfDec), cette enquête propose une analyse approfondie de l'état de la législation sur la protection de la vie privée et des données personnelles en Afrique du Sud, en Éthiopie, au Kenya, en Namibie, au Nigeria, en Tanzanie, au Togo et en Ouganda. Les auteurs ont examiné les engagements régionaux et mondiaux des pays en matière de protection de la vie privée et l'impact de leur environnement législatif sur le droit à la vie privée. Ils ont également procédé à une analyse des lois sur la protection des données, identifié les principaux acteurs et institutions, évalué les pratiques de protection des données dans l'enregistrement des noms de domaine de premier niveau nationaux (ccTLD) sur Internet et examiné le statut de l'autorité de protection des données du pays.

La recherche montre le décalage entre l'adoption officielle du cadre législatif pertinent et la pratique. Sur les huit pays présentés dans le rapport, seuls quatre ont promulgué des lois complètes sur la protection des données personnelles : le Kenya, l'Afrique du Sud, le Togo et l'Ouganda. Cela ne signifie pas pour autant que le pays en question s'engage à faire respecter le droit à la vie privée. Par exemple, le Togo a promulgué une loi sur la protection des données en 2019, et est l'un des rares pays d'Afrique à avoir ratifié la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo). Cependant, des rapports récents montrent la surveillance illégale généralisée des journalistes et des défenseurs des droits humains dans le pays.

Dans la majorité des pays couverts par la recherche, des cadres complets de protection de la vie privée et des données doivent encore être testés, car certaines lois sont nouvelles (adoptées en 2019), ou à l'état de projet.

Le rapport de chaque pays fournit un ensemble de recommandations aux différentes parties prenantes dans les pays respectifs. Un rôle clé pour la société civile identifié dans les recommandations des rapports consiste à surveiller la mise en œuvre des lois sur la vie privée et d'autres législations associées. Aux niveaux local et national, une partie de ce suivi consiste à documenter et à signaler les infractions à la législation sur la protection des données et de la vie privée. Aux niveaux régional et international, il est nécessaire que les groupes de la société civile forment des coalitions afin de renforcer leur capacité de surveillance et de participer activement à des forums tels que l'Examen périodique universel du Conseil des droits humains, lorsque les pays doivent présenter un rapport.

Contribuer et s'engager

MOOC - Droit à la vie privée à l'ère numérique en Afrique

Organisé par le Centre pour les droits humains de l'Université de Pretoria, avec le soutien de Google, ce cours aborde les éléments clés du droit à la vie privée et de la protection des données à l'ère numérique en Afrique. Les concepteurs du cours souhaitaient relever les défis auxquels les pays africains sont confrontés en adoptant une législation adéquate sur la réglementation de la collecte, du contrôle et du traitement des données

personnelles. Le cours a été mis en œuvre en 2021 et rien n'indique à ce jour qu'il aura lieu en 2022.

3.2.2. Chiffrement et sécurité : trouver le juste équilibre

Traditionnellement, seuls les gouvernements avaient le pouvoir et le savoir-faire pour développer et déployer un chiffrement puissant dans leurs communications militaires et diplomatiques. Mais aujourd'hui, grâce à des logiciels conviviaux tels que Pretty Good Privacy (PGP), le chiffrement est désormais à la portée de tout internaute, jusqu'aux criminels et aux terroristes. L'utilisation croissante du chiffrement pose le défi de trouver un juste équilibre entre les droits des utilisateurs de l'Internet à la communication privée et la nécessité pour les gouvernements de surveiller certains types de communication présentant un intérêt pour la sécurité nationale (c'est-à-dire pour contribuer à réduire les activités criminelles et terroristes potentielles).

Les gouvernements et les services de sécurité de nombreux pays tentent d'introduire des limites à la puissance des algorithmes de chiffrement dans les produits et services courants, et d'insérer des portes dérobées qui permettraient aux agences gouvernementales d'accéder aux données chiffrées si cela se révèle nécessaire. Le communiqué conjoint publié en 2017 par les chefs politiques des services de renseignement de l'alliance « Five Eyes » (Canada, Nouvelle-Zélande, Australie, Royaume-Uni et États-Unis) a averti que le chiffrement peut gravement compromettre la sécurité publique, car il empêche l'accès légal au contenu des communications pour les enquêtes sur la criminalité et le terrorisme. Les communautés de la société civile et des droits humains ont exprimé de fortes inquiétudes quant à ces développements, alimentées par les révélations de Snowden, suggérant que les limites au chiffrement et les portes dérobées pourraient être employées pour une censure politique et une surveillance (de masse) disproportionnée. En outre, ces mesures pourraient compromettre l'identité des militants politiques, des blogueurs et des journalistes dans les États autoritaires, mettant ainsi en danger leur sécurité individuelle. Certains chercheurs affirment en fait que l'Internet ne devient pas « clandestin » (« dark », c'est-à-dire chiffré) et que les organismes chargés de l'application de la loi et de la sécurité disposent toujours d'un nombre suffisant de pistes numériques à suivre, sans qu'il soit nécessaire d'affaiblir les systèmes de chiffrement.

Le débat sur un cadre réglementaire international pour le chiffrement est centré sur l'interaction entre des questions complexes concernant la sécurité et les droits humains. Du point de vue de la sécurité, les gouvernements ont réaffirmé la nécessité d'accéder à des données chiffrées dans le but de prévenir la criminalité et de garantir la sécurité publique. Dans ce contexte, des révélations ont été faites sur l'existence de portes dérobées dans des logiciels et des produits chiffrés, et des pressions ont été exercées sur l'Internet et les entreprises technologiques pour qu'ils permettent aux gouvernements d'accéder aux données. En outre, dans certains pays, comme les États-Unis, le Royaume-Uni et la Russie, des efforts ont été déployés pour introduire une législation spécifique exigeant des entreprises technologiques qu'elles autorisent ou aident les organismes chargés de l'application de la loi à accéder aux données et/ou aux appareils chiffrés (dans des circonstances plus ou moins définies).

Du point de vue des droits humains, le droit à la vie privée et les autres droits humains doivent être protégés, et les outils de chiffrement, y compris le chiffrement omniprésent (sur l'ensemble du réseau), sont essentiels pour protéger à la fois la vie privée et la sécurité

personnelle. La nécessité de protéger le chiffrement et l'anonymat a été soulignée, par exemple, dans le rapport 2015 de David Kaye, Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression, sur l'utilisation du chiffrement et de l'anonymat pour exercer les droits à la liberté d'opinion et d'expression à l'ère numérique. Le rapport 2017 de David Kaye traite des rôles que jouent les fournisseurs d'accès à Internet et aux télécommunications. Il passe en revue les obligations des États en matière de protection et de promotion de la liberté d'expression en ligne, puis évalue les rôles de l'industrie de l'accès numérique, et conclut par un ensemble de principes qui guident les démarches du secteur privé pour respecter les droits humains.

Point de réflexion

Le FBI contre Apple

L'affaire du FBI contre Apple, dans laquelle un tribunal fédéral américain a ordonné à Apple d'aider le FBI à déverrouiller l'iPhone de l'un des tireurs qui ont assassiné 14 personnes à San Bernardino en décembre 2015, sert d'exemple à tous les aspects troublants de ce débat. L'affaire a suscité deux points de vue opposés. D'une part, Apple, soutenue par d'autres sociétés Internet et des militants des droits humains, a fait valoir que le fait de se conformer à la demande créerait un dangereux précédent et porterait gravement atteinte à la vie privée et à la sécurité de tous ses clients, comme l'illustre la figure 14. D'autre part, les autorités ont fait valoir que l'affaire n'impliquait pas de portes dérobées ou le déchiffrement d'appareils, mais plutôt une solution ponctuelle, nécessaire dans ce cas particulier. Elles ont également accusé Apple de privilégier ses intérêts commerciaux à une enquête sur le terrorisme.

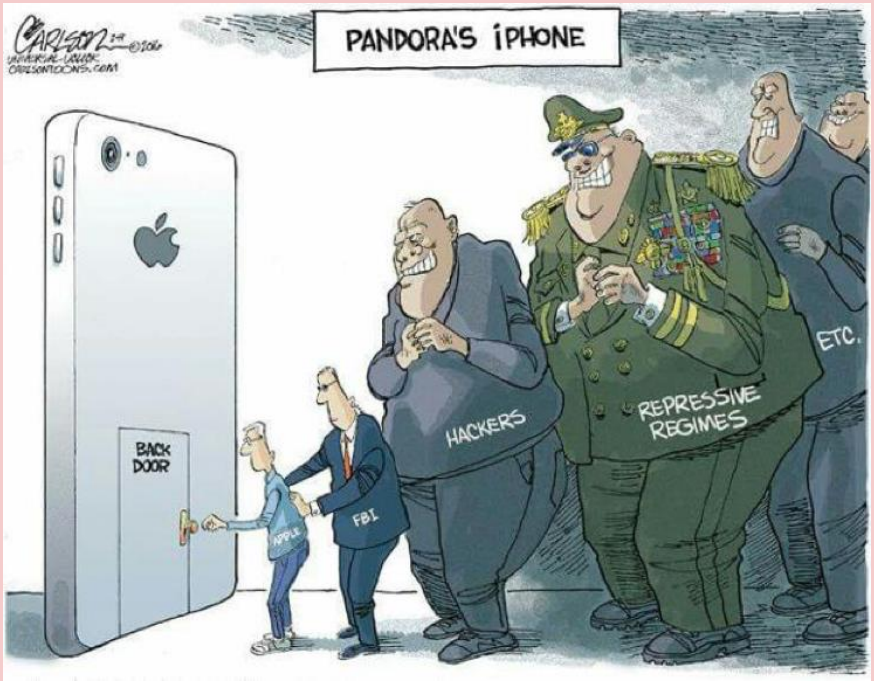


Figure 14. L'iPhone de Pandora
Source : Carlson, 2016

L'affaire a soulevé un certain nombre de questions qui restent ouvertes.

- Dans quelles circonstances les autorités sont-elles habilitées à demander aux entreprises technologiques de revoir à la baisse la sécurité de leurs appareils ?
- Quelles garanties sont, ou devraient être, mises en place ?

- Les autorités devraient-elles être autorisées à influencer la façon dont les entreprises conçoivent leurs produits ?
- Dans le même temps, dans quelle mesure les entreprises doivent-elles protéger la vie privée de leurs utilisateurs ?
- La vie privée doit-elle être protégée à tout prix ?

3.2.3 Liberté d'expression et contenus répréhensibles

Le principe de la liberté d'expression repose sur des normes internationalement reconnues telles que la Déclaration universelle des droits de l'homme, dont l'article 19 prévoit le droit « de chercher, de recevoir et de répandre, sans considérations de frontières, les informations et les idées par quelque moyen d'expression que ce soit ».

Bien que la liberté d'expression soit un droit reconnu, la question du contenu répréhensible est utilisée dans certains cas pour le restreindre. Cela soulève la question de la définition du terme « répréhensible ». Les différentes traditions culturelles et politiques conduisent à une variété de classifications à travers le monde. Ce qui est légal ou acceptable à un endroit peut être illégal ou inacceptable ailleurs. Nous devons donc observer et analyser les problèmes au cas par cas.

Les contenus relatifs aux abus sexuels sur les enfants (CSAM) sont classés comme contenus répréhensibles et illégaux par un consensus mondial et sont donc interdits par le droit international (ius cogens). Néanmoins, de nombreux pays n'ont pas mis en place de réglementations destinées à étendre le champ d'application des lois conventionnelles à la distribution de CSAM ou à l'accès à ces contenus via l'Internet, laissant ainsi l'espace en ligne hors de portée des autorités judiciaires. Toutefois, même lorsque la législation nationale couvre l'espace en ligne, il se peut que les poursuites ne soient pas possibles sans une harmonisation des réglementations au niveau international et une coopération renforcée entre les différentes institutions. Par exemple, la distribution, la possession et l'accès en ligne peuvent être effectués par des personnes résidant en dehors du pays d'impact, donc hors de portée de la juridiction nationale.

La violence, le racisme et les discours de haine sont des types de contenus qui sont « sensibles pour certains pays, régions ou groupes ethniques en raison de leurs valeurs religieuses et culturelles particulières ». La frontière entre contenu répréhensible et liberté d'expression est souvent floue ; les nuances politiques varient d'un État à l'autre. Néanmoins, pour de nombreux pays à travers le monde, les implications de ces contenus ou des activités en ligne de certains groupes ou individus sur la sécurité nationale servent de prétexte pour réprimer la liberté d'expression.

Point de réflexion

Un débat permanent porte sur la question de savoir qui doit être responsable des contenus en ligne, en particulier des discours haineux et extrémistes. Les géants de l'Internet comme Facebook doivent-ils surveiller les contenus ? Le CEO de Facebook, Mark Zuckerberg, affirme qu'ils doivent respecter la liberté d'expression, notamment celle des hommes politiques. Les

réactions sont mitigées, conformément aux positions individuelles sur les discours de haine et la liberté d'expression.

Le Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression, David Kaye, a noté dans son Rapport annuel 2019 qui porte sur les normes juridiques de la lutte contre la haine en ligne et qui a été présenté à l'Assemblée générale des Nations Unies :

> *La prévalence de la haine en ligne pose des défis à tout le monde, et en premier lieu aux personnes marginalisées qui en sont les principales cibles... Malheureusement, les États et les entreprises ne parviennent pas à empêcher que les « discours de haine » ne deviennent la prochaine « fausse nouvelle » [fake news], un terme ambigu et politisé dont abusent les gouvernements et qui se trouve à la discrétion des entreprises.*
>
> également :
>
> *… les nouvelles lois qui imposent une responsabilité aux entreprises ne respectent pas les normes de base, accroissent le pouvoir de ces mêmes acteurs privés sur les normes publiques et risquent de compromettre la liberté d'expression et la responsabilité publique…*

- Cela a-t-il des implications pour la sécurité ou la cybersécurité ?

Étude de cas

L'African Digital Rights Network (ADRN) a réalisé la première étude sur l'ouverture et la fermeture de l'espace civique en ligne dans dix pays africains (Afrique du Sud, Cameroun, Égypte, Éthiopie, Kenya, Nigeria, Ouganda, Soudan, Zambie et Zimbabwe). L'étude a identifié 65 exemples de militants utilisant des outils numériques pour ouvrir un espace civique en ligne, mais presque deux fois plus d'exemples (115) de gouvernements utilisant des outils et des tactiques technologiques pour fermer l'espace en ligne. Il existe des rapports individuels pour chaque pays.

La principale tendance identifiée dans les dix pays est la suivante : chaque nouvelle génération de technologie numérique que les militants utilisent pour exercer la liberté d'expression est confrontée à des mesures gouvernementales sévères, élaborées précisément pour restreindre ces libertés et priver les citoyens de leurs droits numériques.

Par exemple, dans le cas de l'activisme par SMS, qui a été le premier outil numérique utilisé à grande échelle pour créer un espace civique virtuel, il y a eu de nombreux exemples à travers l'Afrique dans lesquels la messagerie texte a été utilisée pour exprimer une dissidence politique, défendre les groupes marginalisés et vulnérables, ou mobiliser les masses. Cette évolution a toutefois été suivie d'une série de mesures répressives telles que l'enregistrement obligatoire des cartes SIM, la surveillance des messages, l'interdiction des SMS groupés et les arrestations pour discours politique par SMS. Un sort similaire a frappé les blogs, les médias sociaux et même les outils de protection de la vie privée et d'anonymisation.

Ressource : Digital Rights in Africa: Challenges and Policy Options

Ce document présente les principaux défis en matière de droits numériques sur le continent, tels que la réglementation régressive des contenus en ligne, les perturbations du réseau et la surveillance, et propose de nombreuses actions et mesures que les acteurs étatiques et non étatiques peuvent employer pour y faire face.

Contribuer et s'engager

Inscrivez-vous au cours en ligne « Introduction à la gouvernance de l'Internet » de Diplo ! Ce cours de dix semaines présente la politique de gouvernance de l'Internet et couvre les principales questions, notamment les droits humains, le développement, l'infrastructure et la normalisation, la cybersécurité, les questions juridiques, économiques et socioculturelles, ainsi que les processus et les acteurs de la gouvernance de l'Internet dans des modules dédiés.

3.3 Aborder la question du genre

Les questions de genre ne sont que rarement abordées dans le cadre de la cybersécurité. Pourtant, nombreuses sont les femmes victimes de la cybercriminalité ou d'autres formes de cyberattaques, telles que le cyberharcèlement, en partie parce qu'elles sont moins sensibilisées que les hommes aux mesures de sécurité lorsqu'elles utilisent l'Internet. De nombreuses organisations commencent à s'attaquer à l'écart existant dans certains pays entre l'accès des femmes et des hommes à l'Internet, et elles veillent à sensibiliser les femmes à l'application de pratiques sûres en ligne. Ce sujet et ses liens avec la cybersécurité doivent être abordés de manière plus significative dans les forums de politique numérique, notamment dans le contexte du discours en ligne et de l'autonomisation des femmes dans l'espace virtuel.

Outre le fait qu'il s'agit d'un sujet important lié aux droits humains, la question du genre a une grave incidence sur la prolifération du commerce électronique en Afrique. Alors que les femmes du continent effectuent la majorité des achats en ligne et hors ligne, elles sont moins susceptibles de posséder un compte bancaire ou d'avoir accès à des cartes de crédit ou à de l'argent mobile. Par exemple, au Kenya, le leader africain en matière de comptes d'argent mobile, la possession d'un compte bancaire chez les femmes est inférieure de 8 % à celle des hommes, tandis que la possession d'une carte de crédit chez les femmes (4 %) est inférieure de moitié à celle des hommes (8 %).

Contribuer et s'engager

L'Observatoire de *veille numérique* GIP suit le thème des droits des femmes en ligne et les questions associées, notamment le fossé numérique entre les sexes, la violence en ligne contre les femmes, etc. Consultez la page pour obtenir des mises à jour quotidiennes sur la question, ainsi que des ressources, des événements et des acteurs associés.

4 Conclusion

Félicitations, vous avez atteint la fin du module. Dans la partie finale, nous réfléchirons aux principaux points à retenir de ce module, en vous laissant un espace supplémentaire pour noter les points qui vous semblent importants et qui ne sont pas inclus ci-dessus.

- La confusion terminologique est grande lorsqu'il s'agit de définir le concept de cybersécurité, allant de différences plutôt mineures comme l'utilisation interchangeable de préfixes (cyber/e/digital/net/virtual) à des différences fondamentales, où l'utilisation de différents termes reflète des approches politiques différentes.

- Les cyberrisques deviennent de plus en plus sophistiqués et les groupes désireux d'exploiter les vulnérabilités du cyberespace sont passés des communautés clandestines de hackers « black hat » à des groupes criminels mondiaux et bien organisés, aux services de sécurité des gouvernements et aux forces de défense nationales. Les outils d'attaque les plus courants sont l'utilisation de logiciels malveillants, ainsi que le spam, les escroqueries en ligne et les techniques d'hameçonnage.

- Parmi les principaux cyberrisques concernant le continent africain figurent les escroqueries en ligne, l'espionnage, les extorsions numériques, la compromission des e-mails d'affaires, les ransomwares et les botnets.

- La cybersécurité ne peut être examinée sans tenir compte d'un contexte plus large et de ses liens avec d'autres questions de gouvernance liées à l'Internet, telles que l'économie numérique et les droits humains en ligne.

- La cybercriminalité a des effets profonds sur le commerce numérique. Aux pertes financières subies du fait de la cybercriminalité s'ajoutent d'autres effets négatifs pour l'économie, comme la diminution de la confiance des consommateurs, la perte de secrets commerciaux et le refus d'accès à certains marchés fréquemment exposés aux cas d'activités frauduleuses.

- Dans le contexte des systèmes nationaux ou internationaux, la discussion sur les droits humains et la sécurité repose souvent une logique binaire : les droits humains et la sécurité ne sont pas compatibles. Il peut sembler que nous devions évaluer ces droits par rapport à des mesures de sécurité, telles que la surveillance ou le contrôle du chiffrement ; pourtant, certaines mesures telles que la promotion de la culture numérique, l'utilisation intelligente des TIC, la promotion de valeurs et la compréhension des technologies numériques et de leur impact sur la société, peuvent renforcer à la fois la sécurité et les droits.