KM6 : Cybercriminalité

Objectifs du module

En matière de criminalité, l'occasion fait toujours le larron. L'Internet offre d'innombrables opportunités. Les délits traditionnels, tels que la fraude, l'usurpation d'identité ou le commerce de biens illégaux, sont désormais perpétrés par le biais de l'Internet. En outre, du fait de l'utilisation accrue des informations personnelles pour les transactions en ligne, il est désormais nécessaire d'équilibrer la sécurité et la vie privée, en particulier en termes d'application de la loi. Ce module explorera les questions relatives à la cybercriminalité, sa définition et son impact, les réponses juridiques et législatives des pays à l'échelle du globe, ainsi que des exemples en Afrique. Le module explorera également la vie privée et la protection des données personnelles à travers un aperçu de l'interaction entre la protection des données et la sécurité. Le module fournira aux participants des connaissances de base sur la façon d'aborder les questions relatives à la cybercriminalité, à la vie privée et à la sécurité.

À la fin de ce module, les participants devraient savoir comment différents pays ont abordé les questions présentées dans le texte et proposer des solutions. Voici quelques-unes des questions qui seront abordées :

- Quelle est la nature de la cybercriminalité ?
- Quelles activités peuvent être assimilées à la cybercriminalité ?
- Quel est l'impact de la criminalité sur l'Afrique ?

- Outre l'impact économique, quels autres domaines sont touchés par la cybercriminalité dans un pays ?
- Quelles sont les réponses à la cybercriminalité ?
- Quelles sont les caractéristiques de la législation relative à la cybercriminalité ?
- Quelle est l'action de la communauté internationale en réponse à la cybercriminalité ?
- Qu'est-ce que la vie privée ?
- Quels sont les principes de la protection des données ?
- Comment concilier les intérêts de la protection des données et de la sécurité ?
- Quelles sont les approches de la protection des données ?
- Que font les pays africains pour protéger la vie privée ?

1. La nature de la cybercriminalité

Il est difficile de donner une définition complète de la cybercriminalité. Certains textes opèrent une distinction entre la cybercriminalité et les délits informatiques. Cette distinction est abordée de manière appropriée dans la publication de l'UIT intitulée Comprendre la cybercriminalité : phénomènes, défis et réponse juridique. Le National Institute of Standards and Technology (NSIT) du Ministère américain du commerce définit la cybercriminalité comme les infractions pénales commises sur l'Internet ou facilitées par l'utilisation de technologies informatiques. Pour notre propos, nous pouvons décrire la cybercriminalité comme un délit, ou un acte illégal commis en utilisant les technologies de l'information et de la communication (TIC). Un tel acte doit être interdit par la loi et des sanctions doivent être prévues. Dans certains cas, les TIC sont utilisées comme un outil alors que, dans d'autres cas, elles sont la cible d'une activité illégale.

Le Crown Prosecution Service (ministère public) du Royaume-Uni, dans sa définition de la cybercriminalité, classe la cybercriminalité en deux catégories. La première catégorie est celle des délits cyberdépendants. Il s'agit de cybercrimes qui sont commis par l'utilisation d'appareils TIC, qui sont à la fois l'outil utilisé pour commettre le délit et la cible du délit. Par exemple, le développement et la propagation de logiciels malveillants à des fins lucratives, le piratage pour voler, endommager, déformer ou détruire des données et/ou un réseau ou une activité. La seconde

catégorie est celle des délits informatiques. Il s'agit de délits traditionnels dont l'ampleur ou la portée peuvent être accrues par l'utilisation d'ordinateurs, de réseaux informatiques ou d'autres formes de TIC, comme la fraude et le vol de données informatiques.

La particularité [1] de la cybercriminalité est que l'Internet a permis l'évolution des délits traditionnels. La copie d'une signature pour retirer des fonds d'un compte bancaire a été remplacée par le vol de numéros de cartes de crédit grâce à l'utilisation massive d'outils en ligne. Le piratage des serveurs, l'infection par logiciels malveillants, la dégradation de sites Web et les attaques par déni de service distribué (DDoS) entrent tous dans la catégorie des nouveaux délits qui sont apparus avec l'Internet.

Le cyberespace offre une abondance d'outils permettant de mener ou de faciliter ces délits, nouveaux ou anciens, tels que les botnets (qui permettent la distribution massive de spam), l'infection par logiciels malveillants, les attaques par déni de service distribué, et bien d'autres. Toute évolution technologique offre aux criminels de nouvelles possibilités de cibler une multitude de victimes potentielles.

Les technologies émergentes modifient également la société, et donc l'environnement dans lequel les délits se produisent. Les développements dans le domaine de l'impression 3D ont permis de produire des armes imprimées entièrement opérationnelles, ainsi que de faux appareils de point de vente (PDV) et des dispositifs de piratage de guichets automatiques destinés à voler les informations des cartes de crédit. Les marchés illégaux sur le « dark Web » sont florissants. Certains d'entre eux (Silk Road 1 et 2, Evolution, Agora et Darkode) ont déjà été démantelés avec succès. Les monnaies numériques (également appelées cryptomonnaies) comme le BitCoin, et les applications d'anonymisation connexes comme Dark Wallet, qui empêchent quasiment le suivi des flux de monnaie numérique, aident les marchés illégaux à échapper plus facilement aux forces de l'ordre.

(https://www.youtube.com/watch?v=2NKvkmGHevc)

Contexte africain

L'Assemblée de l'Union africaine (UA) envisage de négocier un protocole sur le commerce électronique dans le cadre de l'AfCFTA. La pandémie de COVID-19 a accru l'urgence des négociations qui porteront sur les aspects opérationnels du commerce électronique et l'utilisation des outils numériques, notamment la protection, la portabilité, la sécurité et la confidentialité des données ; les flux de données transfrontaliers et les dispositions relatives à la localisation des données ; la coordination des lois sur la cybercriminalité ; et l'harmonisation des lois sur la taxation du commerce électronique transfrontalier.

Source : The Futures Report: Making the AfCFTA Work for Women and Youth

Alors que tout devient « intelligent » et se connecte à l'Internet - des voitures aux ampoules électriques, des réfrigérateurs aux villes intelligentes dans le cadre de l'Internet des objets (IoT) - les appareils intelligents peuvent être assez stupides en matière de sécurité. Les appareils non sécurisés permettent aux criminels d'effectuer diverses actions : ils peuvent les utiliser au sein de botnets, demander une rançon si l'appareil est important (une voiture ou une caméra, par exemple) ou pénétrer plus avant dans le réseau auquel l'appareil est connecté.

Les cybercriminels déploient également l'intelligence artificielle (IA) pour contourner les mesures de sécurité (telles que CAPTCHA), améliorer la précision des attaques d'hameçonnage (phishing) et développer des logiciels malveillants hautement invasifs. L'IA est elle-même une menace, car les appareils autonomes, qui traitent une énorme quantité de données et prennent eux-mêmes les décisions, pourraient être plus vulnérables au piratage, au vol de données personnelles, à l'interception, à la surveillance et à d'autres délits. Trend Micro Research, en collaboration avec l'Institut inter-régional de recherche des Nations unies sur la criminalité et la justice (UNICRI) et le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol, a publié un rapport sur les utilisations malveillantes et les abus de l'intelligence artificielle. Le rapport présente l'état de l'intelligence artificielle et prédit comment les criminels pourraient exploiter ces technologies à l'avenir.

2. L'impact de la cybercriminalité

L'impact des activités des cybercriminels est l'une des raisons pour lesquelles il est nécessaire de s'attaquer à la cybercriminalité. L'évolution de l'environnement évoquée dans la rubrique précédente a parfois entraîné des conséquences désastreuses pour les internautes. Alors que les économies évoluent et dépendent de plus en plus des technologies numériques, les criminels ont également saisi cette opportunité pour leur causer préjudice. Par exemple, la BBC a rapporté que l'attaque de l'oléoduc Colombian Oil aux États-Unis d'Amérique a entraîné le paiement d'une rançon de 5 millions de dollars américains. Le Cybercrime Magazine a estimé que la cybercriminalité entraînerait des pertes annuelles de plus de 10 trillions de dollars américains d'ici à 2025. Cette estimation peut ne pas inclure les incidents non signalés.

Les pays africains sont confrontés à un défi particulier en ce qui concerne l'impact de la cybercriminalité. Il semble que les pays africains soient plus vulnérables aux cyberattaques et à la cybercriminalité. Cela s'explique par l'utilisation accrue des technologies numériques sans les mesures correctives nécessaires en matière de cybersécurité. Dans son article intitulé Cybercrime and Cybersecurity in Africa, Nir Kshetr met en évidence une tendance selon laquelle l'Afrique est la prochaine cible privilégiée des cybercriminels. En effet, la plupart des pays africains sont des marchés émergents et constituent des cibles faciles pour les criminels. Le rapport Interpol d'évaluation des cybermenaces en Afrique en 2021 cite une étude menée par Serianu, société kényane spécialisée dans la cybersécurité informatique, qui souligne que la cybercriminalité a réduit de plus de 10 % le produit intérieur brut (PIB) de l'Afrique, pour un coût d'environ 4,12 milliards de dollars en 2021.

Outre l'économie, il existe d'autres domaines dans lesquels la cybercriminalité peut avoir un impact significatif. Par exemple, le rapport du ministère britannique de la santé sur les cyberattaques WannaCry montre que l'attaque a perturbé au moins 34 % des trusts (unités organisationnelles) du NHS en Angleterre, entraînant l'annulation de près de 19 000 rendez-vous. Dans cinq régions, les patients ont dû « aller plus loin » pour avoir accès à des soins de santé d'urgence. Il s'agissait de circonstances mettant leur vie en danger et susceptibles de faire de nombreuses victimes.

3. Les réponses à la cybercriminalité

L'émergence de la cybercriminalité nécessite des changements importants dans la législation nationale et internationale, afin de donner aux forces de l'ordre les moyens de faire face aux délits impliquant la technologie. Le plus grand défi à la cybercriminalité en termes d'élaboration de la loi est peut-être la nature même de la loi. En règle générale, les lois ne peuvent être appliquées que dans le pays où elles

ont été élaborées . Il est donc difficile d'appliquer les lois sur la cybercriminalité lorsque le criminel se trouve en dehors du territoire concerné . Cependant, la juridiction pénale peut être extra-territoriale par nature lorsqu'une nation l'affirme, soit de manière générale, soit dans des cas spécifiques en vertu de son droit interne. Une autorité supranationale, telle que le Conseil de sécurité des Nations Unies, peut créer un tribunal international destiné à traiter un cas spécifique, comme les crimes de guerre dans un pays donné, ou un tribunal international établi en vertu d'un traité afin de traiter un domaine de compétence déterminé.

Ressources

L'Office des Nations Unies contre la drogue et le crime a mené une étude approfondie et a fourni un rapport en 2013. Ce rapport reconnaît que le développement d'un cadre juridique efficace en matière de cybercriminalité nécessite la prise en compte de certains éléments pour rendre le cadre efficient et efficace. Il s'agit notamment de la mise en place d'un cadre institutionnel, du renforcement des capacités en matière d'application de la loi, du traitement des questions relatives aux preuves électroniques ou numériques, de la coopération internationale et des mesures préventives.

Étude détaillée sur la cybercriminalité de l'UNODC

Guide sur la stratégie de lutte contre la cybercriminalité d'INTERPOL

Ce guide détaillé constitue la ressource pour les pays membres d'INTERPOL qui souhaitent créer ou améliorer leur stratégie nationale en matière de cybercriminalité. Le Guide aide également les pays à mieux comprendre leur réponse actuelle à la cybercriminalité et leur fournit un moyen de concevoir une stratégie et un programme plus solides.

Au fil des ans, de nombreux pays sont parvenus à modifier leur législation existante pour étendre les concepts de divers délits traditionnels au monde numérique et pour ajouter de nouveaux délits. D'autres ont promulgué des lois entièrement nouvelles traitant uniquement de la cybercriminalité. La Conférence des Nations Unies sur le commerce et le développement (CNUCED) fournit une base de données sur la législation en matière de cybercriminalité dans le monde. Cette base de données indique que 80 % des pays se sont dotés d'une législation sur la cybercriminalité, tandis que 5 % en sont encore à des projets de loi. En Afrique (54 pays), 39 pays (72 %) se sont dotés d'une législation sur la cybercriminalité, 2 (4 %) en sont encore

à un projet de législation, 12 (22 %) sont dépourvus de toute législation, et 1 (2 %) n'a pas de données disponibles.

La Figure 1 montre les pays dotés d'une législation sur la cybercriminalité en Afrique.

Source : Base de données de la CNUCED

La législation sur la cybercriminalité identifie les actions préjudiciables et les interdit. Cela crée automatiquement des normes de comportement acceptables pour l'utilisation des TIC. La législation aborde deux aspects distincts : l'aspect matériel, qui prévoit les actes criminels punissables, et l'aspect procédural, qui se concentre sur la collecte des preuves numériques et la poursuite des personnes identifiées pour violation du droit matériel.

Sous l'aspect matériel des législations sur la cybercriminalité, l'objectif est de créer ou de modifier des lois en vue de prévenir les activités illégales faisant appel à l'Internet. Dans certains cas, les lois existantes peuvent être suffisantes pour faire face aux activités illégales en ligne. Dans la plupart des cas cependant, les lois existantes ne permettent pas de gérer les activités préjudiciables en ligne, et il est impératif de créer de nouvelles lois pour criminaliser les activités illicites. Bien qu'il n'existe aucune liste exhaustive des actes de cybercriminalité, l'UIT fournit certaines ressources qui peuvent aider les pays à élaborer une législation appropriée en matière de cybercriminalité.

En Afrique, Maurice a mis au point le système mauricien de signalement en ligne de la cybercriminalité (MAUCORS). Ce système national en ligne permet au public de signaler en toute sécurité les cybercrimes intervenant sur les médias sociaux. Il proposera également des conseils qui permettront de reconnaître et d'éviter les types courants d'actes de cybercriminalité qui se produisent sur les sites de médias sociaux.

L'aspect procédural de la législation en matière de cybercriminalité concerne la collecte de preuves, l'identification des auteurs et les poursuites judiciaires, dans le but d'obtenir une condamnation. Cependant, cet aspect est plus complexe, car les informations sur Internet traversent les frontières sans présenter de documents de voyage. Ainsi, les criminels peuvent aisément contourner les cadres nationaux, s'attaquant à de nombreuses victimes dans différents pays, puisque les données nécessaires à l'enquête criminelle peuvent être stockées chez différents fournisseurs

dans diverses juridictions. La coopération transfrontalière aux niveaux bilatéral, régional et multilatéral est indispensable pour accéder rapidement à ces données.

Contexte africain

La lutte contre la cybercriminalité dans le Commonwealth

Le Secrétariat du Commonwealth gère un projet qui renforce les capacités en matière de cadres juridiques et de prévention de la cybercriminalité. Le projet a commencé en septembre 2020 et se terminera en mars 2023.

Le projet a pour but d'influencer la mise en place de cadres efficaces de lutte contre la cybercriminalité au sein du Commonwealth, à savoir des lois, des politiques, des institutions et des pratiques qui peuvent être exploitées pour combattre le fléau croissant de la cybercriminalité. Les résultats escomptés sont les suivants :

- Sensibilisation accrue ;
- Capacité accrue de lutte contre la cybercriminalité ; et
- Cadres de coopération anti-cybercriminalité renforcés à l'échelle du Commonwealth.

Les pays bénéficiaires de cette phase sont le Botswana, le Cameroun, l'Eswatini, la Gambie et le Ghana.

Les détails de ce projet sont disponibles sur le portail Cybil.

La plupart des accords bilatéraux en matière d'enquêtes criminelles sont conclus par le biais de traités d'entraide judiciaire (MLAT) traditionnels. Ces accords entre pays

visent à recueillir et à échanger des informations et à traiter les questions d'extradition (parfois critiqués pour leur lenteur et leur insuffisance). L'entraide judiciaire exige une double incrimination : un acte doit être criminel dans les deux juridictions lorsqu'un pays demande l'assistance judiciaire d'un autre. Indépendamment du fait que la plupart des pays disposent de lois nationales sur la cybercriminalité, des problèmes peuvent se poser lorsque certains actes punissables dans un pays ne le sont pas dans un autre. Par exemple, le Philippin Onel de Guzman a créé en mai 2000 le ver informatique « Love Bug » qui a infecté plus de 10 millions d'ordinateurs personnels Windows dans le monde, dérobant les mots de passe pour les envoyer à tous les contacts du carnet d'adresses de l'ordinateur. À l'époque, le créateur du ver n'avait pas été poursuivi en justice. En effet, les Philippines ne disposaient pas de loi sur la cybercriminalité et il a bénéficié d'une totale impunité pour ses actions. Des incidents de ce type ont donné lieu à diverses initiatives visant à harmoniser les lois sur la cybercriminalité au niveau mondial.

Par conséquent, plusieurs blocs régionaux ont élaboré des cadres juridiques pour la cybercriminalité afin de permettre les enquêtes au-delà de leurs frontières nationales. Cela a donné lieu à diverses initiatives visant à harmoniser les lois sur la cybercriminalité entre les pays. Il arrive que les pays les plus avancés aident les pays moins développés à mettre en place un cadre juridique et réglementaire en matière de cybercriminalité.

.

Le projet GLACY+

Le projet GLACY+ (Action globale sur la cybercriminalité élargie) est une initiative conjointe de l'Union européenne et du Conseil de l'Europe. GLACY+ s'appuie sur les résultats du premier projet GLACY (2013 – 2016) qu'il vise à étendre et épaule 17 pays prioritaires et plaques tournantes en Afrique, Asie-Pacifique, Amérique latine et dans les Caraïbes. Les pays d'Afrique sont le Bénin, le Burkina Faso, le Cap-Vert, le Ghana, Maurice, le Maroc, le Nigeria et le Sénégal. Ces pays peuvent servir de plaques tournantes pour partager leur expérience en matière de cybercriminalité dans leurs régions respectives.

Source : https://www.coe.int/en/web/cybercrime/glacyplus

Parmi les cadres internationaux, citons notamment la Convention de l'Union africaine sur la cybersécurité et la protection des données de 2014, la loi type du Commonwealth sur la criminalité informatique et liée à l'informatique, l'Accord de la Communauté des États indépendants (2016), l'Accord de l'Organisation de Shanghai pour la coopération dans le domaine de la sécurité internationale de l'information (2009), la Directive européenne sur les attaques contre les systèmes d'information de 2013.

Ces instruments se sont, dans une large mesure, influencés mutuellement, la Convention sur la cybercriminalité du Conseil de l'Europe jouant un rôle de premier plan dans la définition des normes internationales. Cette convention est le document le plus complet et le plus largement accepté en Europe et au-delà, mais elle doit encore surmonter des obstacles pour devenir un accord accepté au niveau mondial. La convention du Conseil de l'Europe sur la cybercriminalité vise à fournir une plateforme pour l'harmonisation des cadres juridiques au niveau mondial. Toutefois, cet objectif se heurte à plusieurs obstacles. Tout d'abord, chaque pays a une compétence territoriale en matière de droit pénal et apporte des perspectives différentes basées sur les traditions et la culture juridiques. Cela conduit au deuxième défi, à savoir que la transposition des dispositions de fond de la convention dans le droit national ne fonctionne pas toujours. En effet, cette transposition peut être en contradiction avec la constitution nationale. Ce qui peut être considéré comme une forme d'art en Australie peut être assimilé à de la pédopornographie au Mali. Tout cadre juridique international relatif à la cybercriminalité doit donc veiller à prendre en compte et concilier ces différences. Si l'harmonisation ne signifie pas la création de lois identiques, il doit y avoir une volonté délibérée de reconnaître les différences entre les lois locales des différents pays. En Afrique, ces facteurs affectent également la Convention de Malabo.

La négociation d'une nouvelle convention mondiale ou régionale peut prendre plusieurs années, voire plusieurs décennies. Il est donc probable que, pour l'instant, les conventions du CdE et de Malabo resteront les accords internationaux et régionaux les plus pertinents en matière de cybercriminalité pour les pays africains.

Parmi les autres initiatives, citons celles menées au niveau des Nations unies (telles que les travaux de l'Union internationale des télécommunications (UIT), de la Commission des Nations unies pour la prévention du crime et la justice pénale (UNCCPCJ) et de l'Office des Nations Unies contre la drogue et le crime (ONUDC)), ainsi que les forums et processus en cours pour la négociation de normes et autres instruments. D'autres parties prenantes, telles que le secteur privé, contribuent

également à la lutte contre la cybercriminalité sous la forme de partage d'informations, d'activités de sensibilisation et de recherches adaptées à leur rôle unique de propriétaires de passerelles vers les infrastructures ou les services Internet.

Ressources

Le référentiel sur la cybercriminalité de l'UNODC propose des ressources qui servent de guide pour l'élaboration de législations sur la cybercriminalité. Il couvre les questions qui doivent être prises en compte dans le droit matériel, le droit procédural et la coopération internationale, entre autres.

Référentiel de l'ONUDC sur la cybercriminalité

Les domaines de coopération ne se limitent pas uniquement aux cadres juridiques et institutionnels. Les Opérations conjointes de lutte contre la cybercriminalité en Afrique (AFJOC) relèvent d'un projet visant à mener des actions coordonnées, fondées sur le renseignement, contre la cybercriminalité et ses auteurs dans les pays membres en Afrique, par la création d'un cadre de coordination régional harmonisé qui produira des plans d'action conjoints et mènera des activités d'application de la loi. L'idée est de s'attaquer aux faiblesses des réseaux et de la sécurité dans un contexte de croissance du marché clandestin et de niveaux élevés d'ingénierie sociale et de menaces à motivation financière contre les personnes vulnérables.

Le concept de cybersécurité est une autre question qui mérite d'être mentionnée lors de l'examen de la cybercriminalité. Si la cybercriminalité concerne la criminalité faisant appel aux TIC, la cybersécurité se concentre sur les mesures que les individus, les organisations et les pays peuvent prendre afin de se protéger contre les cybercriminels et les incidents. L'UIT définit la cybersécurité comme l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement ainsi que les actifs des organisations et des utilisateurs. Le module de connaissances 1a présente les mesures que les pays devraient prendre pour élaborer des stratégies de cybersécurité.

4. L'interaction entre la protection des données et la vie privée

Selon l'International Network of Privacy Law professionals, l'histoire de la protection des données et de la vie privée remonte à 1890, lorsque deux avocats américains, Samuel D. Warren et Louis Brandeis, ont rédigé l'article « The Right to Privacy ». Cet article affirmait que les gens devaient avoir le « droit d'être laissés en paix », utilisant cette expression comme définition de la vie privée. Le premier document juridique à prévoir ce droit est la Déclaration universelle des droits de l'homme de 1948, qui a adopté comme douzième droit le « droit à la vie privée ». Depuis, de nombreux pays ont inclus ce droit parmi les droits fondamentaux de leurs citoyens. Par exemple, la Constitution sud-africaine contient le droit à la vie privée dans son Article 14, la Constitution marocaine dans son Article 24, et la Constitution ghanéenne dans son Article 18.

Le droit à la vie privée est un droit garanti par la loi et c'est un droit fondamental qui est accordé aux individus parce qu'ils sont des êtres humains. La protection des données, quant à elle, est définie par l'Oxford Dictionary comme un ensemble de contrôles juridiques visant à préserver la confidentialité des informations stockées sur les ordinateurs et à limiter les personnes qui peuvent les lire ou les utiliser. Dans le cas de la protection des données, qui se rapporte à la vie privée, l'accent est mis sur les informations personnelles. La protection des données et la vie privée sont donc toutes deux créées par des régimes juridiques. Selon la Conférence des Nations unies sur le commerce et le développement (CNUCED), 128 des 194 pays du globe ont mis en place une législation visant à garantir la protection des données et de la vie privée. En Afrique, seuls 29 pays sur 54 ont établi un régime juridique pour la protection des données. Certains ont commencé à élaborer des lois.

L'interprétation de la vie privée reflète des perceptions différentes. Ces perceptions incluent des droits tels que le droit de ne pas être observé, le droit d'être laissé en paix, le droit de garder secrètes ses pensées, ses convictions, son identité et son comportement, le droit de choisir et de contrôler quand, pourquoi, où, comment et à qui révéler des informations sur soi-même, quelles sont ces informations et dans quelle mesure elles sont révélées. Ce droit est directement lié au droit à la liberté d'expression et d'association. L'anonymat est nécessaire pour protéger les droits d'un individu.

De nombreux utilisateurs choisissent d'accéder à l'Internet de manière anonyme, pour diverses raisons. Le concept Tor (tout ou rien) est un outil qui aide à préserver l'anonymat des utilisateurs. Ce logiciel ouvert a été développé pour protéger la vie

privée et la liberté individuelle par l'anonymisation et la prévention de l'analyse et de la surveillance du trafic. À l'instar de divers outils de cryptage, le concept Tor garantit la sécurité et peut même sauver la vie de militants et de journalistes travaillant dans des régions du monde politiquement instables.

Cependant, l'absence d'identification a créé un environnement permettant aux criminels d'agir dans l'anonymat. Elle a également poussé certaines personnes à communiquer à d'autres des propos cruels, discriminatoires, racistes, haineux et/ou d'autres formes de discours offensant, ce qu'elles n'auraient pas fait si leur identité avait été connue. Cela constitue un défi pour les agences de sécurité et les organismes d'application de la loi.

Ces dernières années, les révélations de Snowden sur l'utilisation de programmes de surveillance par l'Agence de sécurité nationale des États-Unis (NSA), les révélations ultérieures sur la surveillance exercée dans divers autres pays, ainsi que l'augmentation de la cybercriminalité et du terrorisme, ont mis en lumière les droits de l'homme dans le contexte de la sécurité.

Dans la perspective des droits de l'homme, il est impératif de protéger le droit à la vie privée et les autres droits de l'homme. Les outils de cryptage, dont le cryptage généralisé, sont essentiels à la protection de la vie privée. Du point de vue de la sécurité, cependant, les gouvernements ont réaffirmé la nécessité d'accéder à des données cryptées dans le but de prévenir la criminalité et de garantir la sécurité publique. Cet impératif a exercé une pression croissante sur les sociétés Internet et technologiques pour qu'elles permettent aux gouvernements d'accéder aux données.

L'interaction entre le cryptage, la protection de la vie privée et la lutte contre la cybercriminalité (sans oublier la manière d'équilibrer toutes ces questions) a fait l'objet d'un débat animé lorsque, en août 2021, Apple a annoncé de nouvelles mesures visant à analyser les photos iCloud (les photos des utilisateurs) pour y déceler la présence de matériel pédopornographique (CSAM). Ces mesures ont été mises en attente, sur la base d'au moins deux problèmes : le premier était que la capacité d'Apple à analyser les photos iCloud constituait en soi une violation de la vie privée ; le second était que les gouvernements pouvaient vouloir contraindre Apple à utiliser cet outil à leurs propres fins non démocratiques. À la lumière de ces préoccupations, les parties prenantes débattent toujours de la marche à suivre.

Dans une économie fondée sur l'information ou les données, on ne saurait trop insister sur la valeur des données personnelles. Les données sont utilisées pour développer des modèles commerciaux, fournir une plateforme efficace pour la commercialisation de biens et de services, comprendre les préférences des consommateurs et développer des produits et des services. Toutefois, les données sont neutres, à l'instar de la technologie, et elles peuvent également être utilisées à des fins malveillantes. Des cas très médiatisés de fuites de données ont été enregistrés chez Facebook, eBay, Equifax et Uber. Des centaines de millions d'informations personnelles de particuliers (numéros de sécurité sociale, adresses, cotes de crédit, etc.) ont été compromises. Afin d'aborder la question de la vie privée et de la sécurité, en équilibrant les droits fondamentaux des citoyens et la menace des cyberdélits, plusieurs pays ont élaboré des lois et des réglementations afin de donner aux citoyens des droits sur leurs données personnelles et de réglementer l'accès à ces données et leur utilisation, notamment par les organismes en charge de l'application de la loi.

La plus populaire de ces lois est sans doute le Règlement général sur la protection des données (RGPD) de l'Union européenne. Cette loi crée pour les organisations et les entreprises des règles régissant l'utilisation des données personnelles en toute intégrité. La loi définit des principes pour le traitement des données personnelles, tels que le traitement de manière légale, équitable et transparente, la limitation de la finalité, des données et du stockage, prévoit les droits de la personne concernée et garantit la protection de la vie privée dès la conception. Reconnaissant l'absence de frontières sur Internet, le RGPD définit la compétence territoriale de la loi pour les entreprises établies dans l'Union européenne et les entreprises situées en dehors de l'Union européenne qui offrent des biens ou des services aux résidents de l'UE ou surveillent leur comportement. Cette perspective élargit le champ d'application de la loi.

Un autre domaine intéressant qui mérite d'être mentionné est la directive de l'UE relative à l'application des lois sur la protection des données. En général, la pratique en vigueur dans la plupart des régimes juridiques de protection des données consistait à exclure de l'application de la loi les activités répressives, en particulier les enquêtes criminelles et les questions touchant à la sécurité nationale. Cependant, la plupart des pays ont reconnu que même lorsque les citoyens font l'objet d'une enquête, ils jouissent toujours de certains droits, notamment en ce qui concerne le traitement de leurs données. Sur cette base, les pays commencent à créer des règles spéciales pour les services d'application de la loi, afin de maintenir

un certain niveau de droits à la vie privée pour les citoyens, même lorsqu'ils font l'objet d'une enquête criminelle.

Meilleures pratiques

Les principes de protection de la vie privée et des données des Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontaliers de données de caractère personnel de 2013 fournissent un modèle pour les principes de protection des données, qui a été adopté par les lois sur la protection des données dans diverses juridictions. Ces principes sont les suivants :

Principe de limitation de la collecte : la collecte de données personnelles doit être limitée conformément à la loi et, le cas échéant, au consentement de la personne concernée.

Principe de qualité des données : les données personnelles doivent être exactes et pertinentes au regard de la finalité pour laquelle elles sont destinées à être utilisées.

Principe de spécification de la finalité : la finalité de la collecte doit être spécifique et les données ne doivent être utilisées qu'à cette fin.

Principe de limitation de l'utilisation : les données personnelles, lorsqu'elles sont collectées dans un but précis, ne doivent être utilisées que dans ce but, sauf avec le consentement de la personne concernée ou en vertu de la loi.

Principe des garanties de sécurité : les données personnelles doivent être protégées par des mesures de sécurité raisonnables contre des risques tels que la perte ou l'accès, la destruction, l'utilisation, la modification ou la divulgation non autorisés des données.

Principe d'ouverture : il doit y avoir une politique générale d'ouverture concernant les développements, les pratiques et les politiques en matière de données personnelles.

Principe de participation individuelle : la personne concernée a des droits qui peuvent inclure

le droit de les obtenir auprès d'un contrôleur de données, ou de confirmer que le contrôleur de données possède des données la concernant ; d'obtenir la communication des données la concernant dans un délai raisonnable et, le cas échéant, moyennant des frais raisonnables, d'une manière raisonnable ; et sous une forme qu'elle puisse aisément comprendre ; d'être informée des raisons pour lesquelles une demande d'information concernant ses données est rejetée, et de pouvoir contester ce rejet ; et de contester les données la concernant et, si la

contestation aboutit, d'obtenir que ces données soient effacées, rectifiées, complétées ou modifiées.

Principe de responsabilité

Un contrôleur de données devra s'assurer du respect des mesures qui donnent effet aux principes énoncés ci-dessus.

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel stipule que les parties s'engagent, en vertu de l'Article 8.1, à *mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute atteinte à la vie privée, sans préjudice du principe de liberté de circulation des données à caractère personnel*. L'Article 11.1 de la Convention exige que chaque État Partie *mette en place une autorité chargée de la protection des données à caractère personnel*.

L'Information Regulator (Afrique du Sud) est établi en vertu de la loi sur la protection des informations personnelles de 2013 (POPIA Act). Les membres de l'Information Regulator (Afrique du Sud) ont entamé un nouveau mandat à dater du 1er décembre 2021, suite à une nomination par le président. Les nouveaux membres ont été nommés après la prise en charge par le régulateur des fonctions prévues par la loi de 2000 sur la promotion de l'accès à l'information (PAIA) et l'entrée en vigueur des pouvoirs d'application prévus par la loi de 2013 sur la protection des informations personnelles (POPIA).

La loi sur la protection des données établit l'*Agência de Proteção de Dados* (APD) comme autorité de protection des données en Angola. Le statut organique de l'APD a été établi par le décret présidentiel 214/2016.

Le Bureau du commissaire pour la protection des données (Office of the Data Protection Commissioner - ODPC) du Kenya a été créé en 2020 suite à la promulgation de la loi sur la protection des données de 2019. La loi devrait être soutenue par le Règlement (général) sur la protection des données de 2021, qui définit les procédures à suivre pour faire respecter les droits des personnes

concernées, tout en précisant les devoirs et obligations des responsables du contrôle et du traitement des données. Les Règlements sur la protection des données (conformité et application) de 2021, qui décrivent les dispositions de conformité et d'application pour le Commissaire aux données, ainsi que pour les responsables du contrôle et du traitement des données et les Règlements sur la protection des données (enregistrement des responsables du contrôle et du traitement des données) de 2021 définissent la procédure qui sera adoptée par le Bureau du Commissaire pour la protection des données pour enregistrer les responsables du contrôle et du traitement des données.

Le Réseau africain des autorités de protection des données rassemble les organismes de réglementation de la protection des données en Afrique. Il a été mis en place à Ouagadougou, au Burkina Faso, en septembre 2016, lors d'un événement parallèle au forum africain sur la protection des données personnelles. Il regroupe actuellement plusieurs autorités africaines de protection de la vie privée et des données, issues de différentes zones géographiques et linguistiques, dans le but de mettre en place une plateforme d'échanges et de coopération entre ses membres et de faire entendre la voix de l'Afrique auprès de ses partenaires du monde entier. Les membres sont les suivants : Afrique du Sud, Angola, Bénin, Burkina Faso, Cap-Vert, Gabon, Ghana, Kenya, Mali, Maroc, Maurice, Niger, Nigeria, Ouganda, Sao Tomé-et-Principe, Sénégal, Tchad et Tunisie. Veuillez noter que l'Organisation internationale de normalisation (ISO) dispose d'une norme relative à la confidentialité des données. Il s'agit de la norme ISO 27701.

Enfin, ces derniers temps ont vu l'émergence d'une question concernant le contrôle et le mouvement des données en général. Cette question affecte invariablement les données personnelles et la vie privée. L'émergence du cloud computing a créé une plateforme pour le stockage omniprésent des données. Ainsi, le traitement des données peut avoir lieu virtuellement, sans reconnaissance des frontières géographiques ou nationales. La nécessité pour les gouvernements de suivre le rythme de la collecte, de la circulation et du contrôle des données a conduit à des politiques qui affectent le flux d'informations sur l'Internet.

Des concepts tels que la souveraineté des données, la résidence des données et la localisation des données tentent de réglementer l'emplacement physique des données. La souveraineté des données fait référence au principe selon lequel les données, quel que soit l'emplacement où elles sont stockées, doivent respecter les lois d'un pays souverain spécifique. La résidence des données fait simplement référence à une situation dans laquelle la loi spécifie l'emplacement physique des

données. La localisation des données fait référence à une exigence administrative ou juridique obligatoire, selon laquelle les données doivent être stockées ou traitées, de manière exclusive ou non exclusive, dans une juridiction donnée.

L'argument en faveur de la localisation des données repose sur quelques points, à savoir l'intérêt de la sécurité nationale ; la protection des données personnelles et l'application des lois sur la protection des données ; la garantie d'un accès plus rapide et plus sécurisé aux données pour l'application de la loi ; la promotion de la compétitivité économique locale ; l'augmentation de la croissance économique et la stimulation de l'emploi ; et la prévention de la surveillance étrangère.

Au niveau international, plusieurs pays ont créé des régimes de localisation des données. La Russie exige la localisation des données pour toutes les données personnelles. Le Kazakhstan exige que toutes les données soient stockées sur les serveurs du domaine spécifique du pays (.kz).[8] [9] L'Australie exige que les dossiers médicaux soient stockés localement. Le Canada exige des fournisseurs de services publics qu'ils respectent les exigences en matière de localisation des données. La Chine a, en matière de localisation des données, des exigences qui s'appliquent à toutes les données personnelles, commerciales et financières. Les exigences de l'Inde en matière de localisation des données s'appliquent aux fournisseurs de services de paiement et aux marchés publics. Les États-Unis exigent que les données relatives aux citoyens du pays soient traitées et/ou conservées dans ce pays. Les données couvertes par ces lois peuvent aller de toutes les données à caractère personnel à des types de données spécifiques comme les informations sanitaires ou financières.

Cependant, l'Indian National Institute of Public Finance and Policy affirme que l'hypothèse selon laquelle la localisation des données conduira nécessairement à une meilleure protection de la vie privée est erronée. En effet, la sécurité des données est davantage déterminée par les mesures techniques, les compétences, les protocoles de cybersécurité mis en place que par leur simple localisation. Globalement, le degré de protection des données dépendra de l'efficacité du régime de protection des données applicable, et non de la localisation des données.

5. Principaux enseignements

L'utilisation des TIC s'est considérablement développée car elle offre aux entreprises et aux pays la possibilité de travailler efficacement et de promouvoir la croissance

économique. Cependant, la technologie étant neutre, elle offre également aux criminels la possibilité de perpétrer leurs activités illégales. Cette menace, généralement appelée cybercriminalité, doit être traitée par des cadres juridiques et institutionnels.

Ce module a mis en lumière les définitions de la cybercriminalité, les initiatives et les concepts qui s'y rapportent, ainsi que les défis à relever pour enrayer les activités illégales en ligne. Le module a abordé l'impact économique de la cybercriminalité, les approches déployées en Afrique et à l'international pour traiter les questions de cybercriminalité, et les ressources disponibles à l'intention des pays qui souhaitent développer des cadres juridiques pour la cybercriminalité. Le texte mentionne par ailleurs les différents cadres régionaux et internationaux, ainsi que les défis liés à la mise en œuvre de ces cadres.

Le module a également abordé la vie privée, la protection des données et la sécurité nationale dans le contexte des droits de l'homme. Des questions telles que le contenu de base des cadres juridiques pour la protection des données, les conseils pour l'élaboration de ces cadres et l'application des principes de base de la vie privée basés sur les droits de l'homme fondamentaux.

Les questions identifiées dans ce module doivent servir de guides pour d'autres actions ou activités concernant les régimes juridiques afin de traiter la cybercriminalité, la vie privée et la protection des données.