سلطنة عمان
وزارة التربية والتعليم

EMC
مسقط 2024
Muscat 2024

إيسيسكو
ICESCO

Conférence de l'ICESCO des Ministres de l'Éducation

ICESCO EMC 3

Au-delà du Sommet sur la Transformation de l'Éducation: des Engagements aux Actions

3.5

Éducation numérique

Mascate,
Sultanat d'Oman

2-3 octobre 2024

سلطنة عمان
وزارة التربية والتعليم

EMC
مسقط 2024
Muscat 2024

إيسيسكو
ICESCO

Conférence de l'ICESCO des Ministres de l'Éducation

ICESCO EMC 3

Au-delà du Sommet sur la Transformation de l'Éducation :
des Engagements → aux Actions

3.5

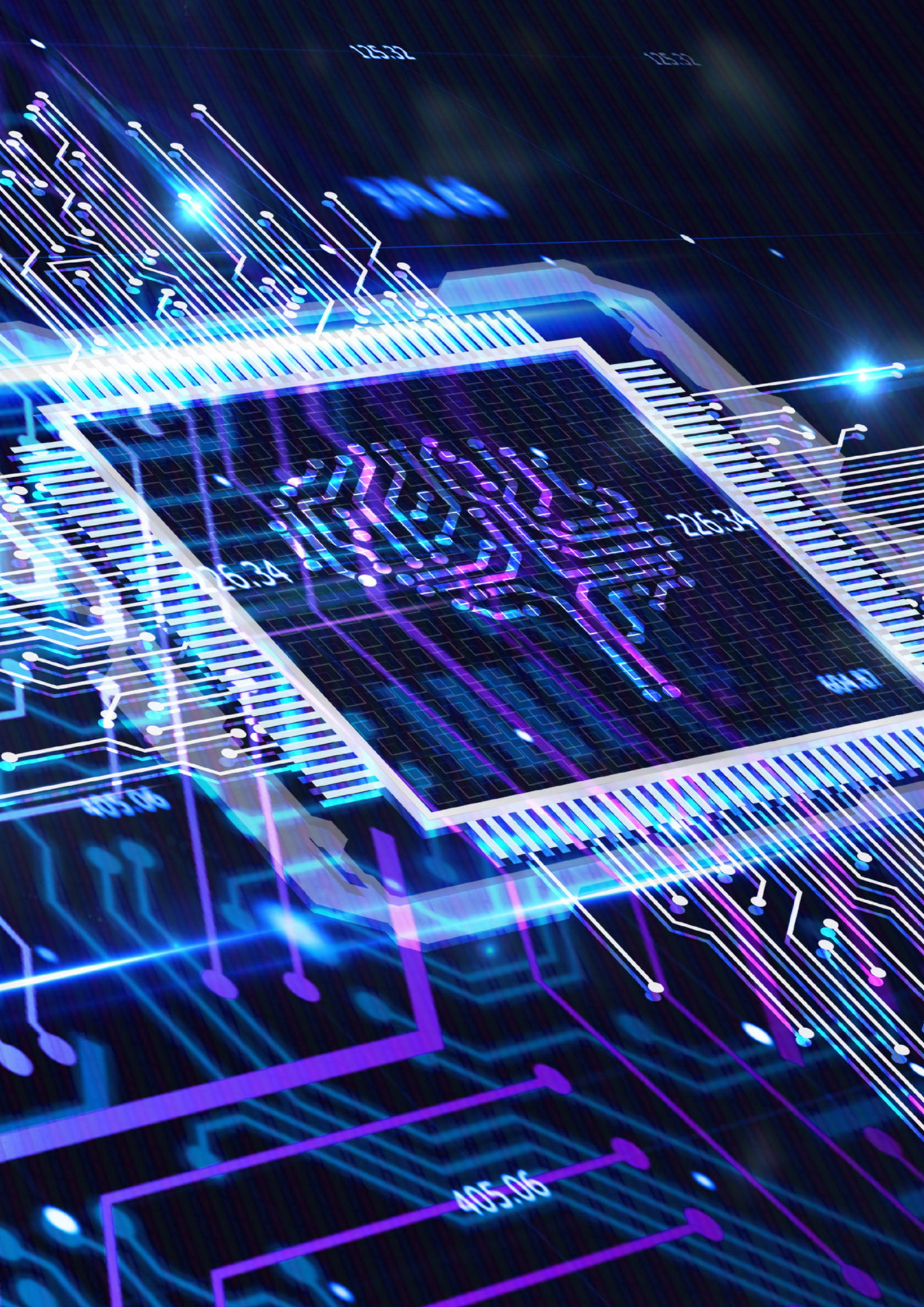
Éducation numérique

Mascate,
Sultanat d'Oman

2-3
octobre

2024

SOMMAIRE


125.32
125.32
26.34
26.34
405.06
405.06

0

AVANT PROPOS

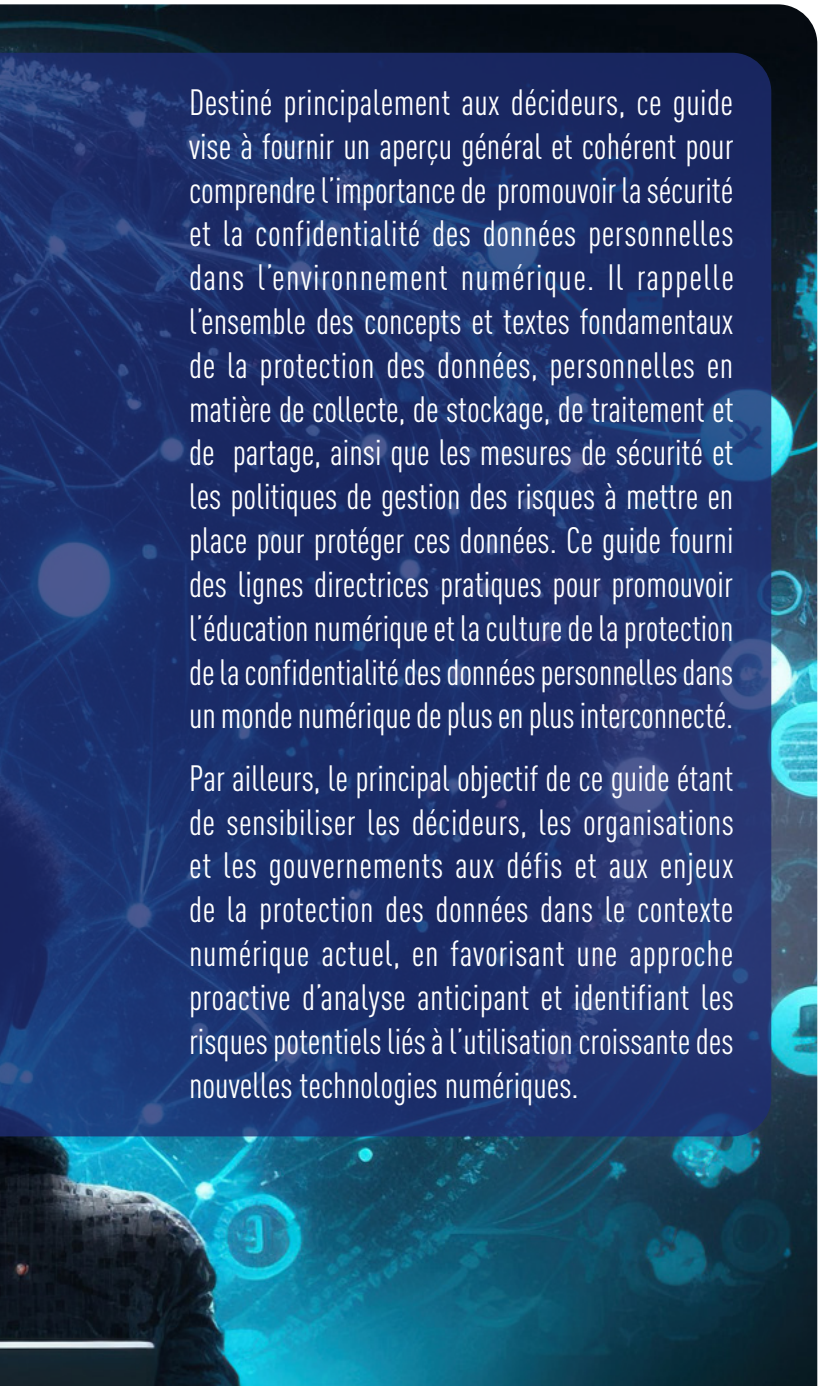
AVANT PROPOS

Dans la contemporanéité, avec l'avènement de la technologie numérique et de l'intelligence artificielle, l'humanité devient de plus en plus immergée dans un environnement numérique qui ne cesse de façonner le quotidien des individus de multiples manières et sur diverses dimensions. Certes, les opportunités que procure cet environnement numérique, notamment dans le domaine de l'éducation, sont bien documentées et prouvées, cependant, ce même environnement peut être la source d'un certain nombre de risques mettant en jeu le bien-être de ses utilisateurs et leur jouissance de leurs droits humains, la violation et l'exploitation des données personnelles, entre autres, constitue l'un de ces risques.

A cet effet, les décideurs politiques et les praticiens, y compris les législateurs, les autorités de contrôle ainsi que l'industrie de la technologie numérique devraient promouvoir des lignes directrices et mettre en œuvre des mesures pour respecter les obligations en matière de protection des données et de la vie privée. Les intervenants concernés et les parties prenantes doivent être conscients de cette problématique à ampleur grandissante comme ils sont appelés à mettre en place et en œuvre des mesures et des directives solides visant la protection des données : Des mesures fournissant des pratiques saines de gestion et de protection des données personnelles devant toute entité impliquée dans le traitent et l'usage des données à caractère personnel et des mesures qui puisent dans les normes et les principes des politiques et des lois internationales et locales permettant la protection des données personnelles et l'inculquant en tant que culture.

Ce guide a été conçu et rédigé pour aider les décideurs afin d' éclairer leur prise de décision en matière de la protection des données. Il met en évidence les principaux changements, défis et actions que les organisations doivent adopter pour atteindre la conformité normative et critériée en cette matière.

A. Objectifs du guide



Destiné principalement aux décideurs, ce guide vise à fournir un aperçu général et cohérent pour comprendre l'importance de promouvoir la sécurité et la confidentialité des données personnelles dans l'environnement numérique. Il rappelle l'ensemble des concepts et textes fondamentaux de la protection des données, personnelles en matière de collecte, de stockage, de traitement et de partage, ainsi que les mesures de sécurité et les politiques de gestion des risques à mettre en place pour protéger ces données. Ce guide fourni des lignes directrices pratiques pour promouvoir l'éducation numérique et la culture de la protection de la confidentialité des données personnelles dans un monde numérique de plus en plus interconnecté.

Par ailleurs, le principal objectif de ce guide étant de sensibiliser les décideurs, les organisations et les gouvernements aux défis et aux enjeux de la protection des données dans le contexte numérique actuel, en favorisant une approche proactive d'analyse anticipant et identifiant les risques potentiels liés à l'utilisation croissante des nouvelles technologies numériques.

En outre, ce guide vise à promouvoir une culture de responsabilité et de transparence dans la gestion des données personnelles, en encourageant les organisations à adopter des politiques et des pratiques conformes aux normes internationales et aux réglementations en vigueur en matière de protection des données, et en mettant en place un mécanisme de coopération et un cadre de collaboration entre les parties prenantes des Etats membres de l'ICESCO, afin de promouvoir l'échange d'informations et des bonnes pratiques, l'encouragement de la collaboration et le partage d'expériences entre les acteurs de l'écosystème numérique, favorisant ainsi le renforcement des synergies dans le domaine de la protection des données, le développement des normes communes, le renforcement de capacités, et aussi la mise en conformité aux normes de base en matière de protection des Données.

B. Importance de la sécurité des données personnelles

Dans l'écosystème complexe actuel de la société de l'information et de la communication, la protection des données personnelles joue un rôle crucial à plusieurs niveaux. Tout d'abord, elle est essentielle pour préserver la vie privée des individus dans un environnement où les données personnelles sont échangées à une échelle sans précédent. Cette protection est indispensable pour garantir que les individus conservent le contrôle sur leurs informations en évitant toute forme d'exploitation.

Ensuite, la protection des données est un pilier fondamental et rassurant de la confiance numérique. En instaurant des normes de sécurité et de confidentialité robustes, on favorise un climat de confiance entre les utilisateurs, les entreprises et les gouvernements, ce qui est essentiel pour promouvoir l'adoption généralisée des technologies de l'information et de la communication (TIC) et stimuler ainsi l'innovation et la croissance économique.

De plus, dans un monde où les cybermenaces sont omniprésentes, la protection des données est une composante essentielle de la cybersécurité. Ainsi, la mise en place des mesures de protection adéquates, permet de prévenir les violations de données et les actes de cybercriminalité qui pourraient compromettre la stabilité et la sécurité de la société de l'information.

Aussi, la protection des données est un enjeu éthique et politique majeur, soulevant des principales questions sur la protection de la vie privée, la promotion des libertés individuelles et l'instauration de la responsabilité sociale des entreprises et des gouvernements. En veillant à ce que les données soient utilisées de manière éthique et responsable, elle contribue à préserver les valeurs démocratiques et les droits fondamentaux dans un environnement numérique en constante évolution.

Finalement, la protection des données personnelles est un impératif moral, économique et social qui nécessite une attention continue et un engagement concerté de la part de toutes les parties prenantes.

C. Rôle de l'Education numérique

L'éducation numérique joue un rôle essentiel dans la promotion de la protection des données personnelles. Elle sensibilise les individus aux enjeux de confidentialité et de sécurité liés à la manipulation des données personnelles dans un environnement numérique. En fournissant aux individus les connaissances et les compétences nécessaires pour comprendre les principes fondamentaux de la protection des données, elle les équipe pour leur permettre de naviguer sereinement dans le monde digital, tout en prenant des décisions éclairées sur la manière de fournir gérer, et protéger leurs informations et données personnelles.

L'éducation numérique, forme les jeunes utilisateurs aux bonnes et meilleures pratiques en matière de protection des données personnelles.

Cela passe par l'intégration des concepts de la protection des données personnelles et de la vie privée dans les programmes scolaires afin de doter les apprenants de compétences sur la sécurité des données et de la confidentialité dans l'espace numérique.

Par ailleurs, l'éducation numérique sur les données personnelles, encourage le développement de solutions digitales innovantes pour renforcer la protection des données. En stimulant la recherche et le développement dans le domaine de la cybersécurité et de la protection de la vie privée, elle favorise l'émergence de nouvelles approches et de nouveaux outils pour garantir la sécurité et l'intégrité des données personnelles dans un monde numérique en constante évolution.

Enfin, l'éducation numérique instaure une culture de responsabilité et de citoyenneté numérique. Elle se traduit par une double approche ; le principe du droit à la vie privée et à la protection des données de chaque citoyen, mais également la responsabilité qui incombe à chaque utilisateur, celui de protéger ses propres données personnelles ainsi que celles des autres, quand cela est possible.

La formation et l'apprentissage de l'éducation numérique permettra ainsi de créer un environnement en ligne plus sûr, plus éthique, plus inclusif, plus responsable et plus équitable pour tous les utilisateurs..

D. Cas des pays membres de l'ICESCO

Le respect de la vie privée est un droit humain protégé en vertu de l'article 12 de la Déclaration Universelle des droits de l'homme ainsi que de l'article 17 du Pacte international relatif aux droits civils et politiques. Les Etats membres de l'ICESCO et non membres disposent de lois sur la protection des données qui renforcent la protection de la vie privée. Plus de 132 pays à travers le monde ont déjà élaboré et adopté des lois de protection des données, fondées sur les normes internationales.

La protection des données personnelles dans les Etats membres de l'Organisation du Monde Islamique pour l'Education, les Sciences et la Culture (ICESCO) est devenue une préoccupation croissante dans un contexte de transformation numérique rapide des sociétés.

Malgré les disparités entre les Etats membres, en matière de politiques, de stratégies et des systèmes de protection des données personnelles, l'ensemble des pays ont pris conscience de l'importance cruciale de la protection des données personnelles, de la vie privée et de la confidentialité des individus dans un environnement numérique. Les Etats membres de l'ICESCO ont commencé à élaborer des cadres juridiques et réglementaires pour garantir la protection des données personnelles conformément aux normes internationales et aux principes islamiques.

Des efforts ont été consentis pour privilégier une coopération régionale, interrégionale et internationale afin de réfléchir sur la manière d'aborder ces préoccupations, de créer des dynamiques d'échanges et de collaboration qui servent l'émergence d'environnements sains et inclusifs dans les Etats membres de l'ICESCO.

Ainsi, ce guide rappelle d'une manière non exhaustive , les efforts des Etats membres de l'ICESCO sur le plan juridique et organisationnel, à savoir la mise en place des textes de lois relatifs à la protection des données personnelles, et l'élaboration des mécanismes de contrôle, assurant le respect des lois et des réglementations en la matière, et l'encouragement de la sensibilisation et la formation des professionnels et des citoyens sur les enjeux de la vie privée et de la sécurité des données personnelles, afin de renforcer leur capacité à protéger leurs informations personnelles.

1

“PROTECTION DES DONNÉES PERSONNELLES, CADRE LÉGAL ENJEUX, FONDAMENTAUX”

A. DIFFÉRENTES DÉFINITIONS DES DONNÉES PERSONNELLES

B. FONDAMENTAUX DE LA PROTECTION DES DONNÉES PERSONNELLES

C. ÉVOLUTION DES PRATIQUES DE COLLECTE, DE TRAITEMENT ET D’UTILISATION DES DONNÉES PERSONNELLES

D. ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES, RISQUES ET CONFIANCE NUMÉRIQUE.

A. DIFFÉRENTES DÉFINITIONS DES DONNÉES PERSONNELLES

Il existe différentes définitions des données personnelles ou à caractère personnel, selon les contextes juridiques et réglementaires, voici quelques-unes des définitions courantes :

D'après l'article 4, du Règlement Général sur la Protection des Données (RGPD[1] de l'Union Européenne, une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Cela inclut des informations telles que l'adresse IP, les données biométriques, etc.

Tandis que la loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) [2], au Canada, définit les données personnelles comme des informations ou plus tôt renseignements relatifs à un individu identifiable, à savoir des renseignements trait à sa santé physique ou mentale.

La Loi sur la protection des données (DPA)[3] au Royaume-Uni, définit les données personnelles

comme toute donnée qui aurait pu être utilisée pour identifier un individu vivant. Les données anonymisées ou agrégées étaient moins réglementées par la loi, à condition que l'anonymisation ou l'agrégation n'ait pas été effectuée de manière réversible. Cela peut inclure des données telles que le nom, l'adresse, l'adresse e-mail, le numéro de téléphone, les données médicales, les données financières, etc.

Aux États-Unis, Le CCPA California Consumer Privacy Act [4], à l'instar des autres Etats, définit les données personnelles comme toute information qui identifie, se rapporte à, décrit, est capable d'être associée à, ou pourrait raisonnablement être liée, directement ou indirectement, à un consommateur ou à un ménage. Le CCPA garantit les droits à la vie privée et la protection des consommateurs résidant en Californie en ce qui

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données.

[2] Loi canadienne sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5)

[3] DPA: Data Protection Act 2018, nouvelle loi du Royaume Uni sur la protection des données, a reçu le sceau royal le 23 mai, deux jours avant la date d'entrée en vigueur de 2016/679 (¨RGPD¨).

[4] CCPA: California Consumer Privacy Act est la loi sur la protection des données, visant à protéger les informations personnelles identifiables (IPI) des résidents de Californie des Etats-Unis, promulguée en 2018, entrée en vigueur en 2020.

concerne leurs informations personnelles identifiables. Le CCPA vise à renforcer la protection de la vie privée des consommateurs en Californie en imposant des obligations aux entreprises qui collectent et traitent les données personnelles.

Parmi les données personnelles, il existe la catégorie des données dites « sensibles » qui sont des informations qui, en raison de leur nature, une fois divulguées, peuvent présenter un risque accru pour la vie privée et la sécurité physique ou morale des individus. Ces données comprennent généralement des informations relatives à l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, l'état de santé ou la vie sexuelle. En raison de leur caractère délicat, ces données requièrent souvent une protection renforcée et sont généralement soumises à des restrictions plus strictes en matière de collecte, de traitement et de partage conformément aux lois et réglementations en vigueur.

Dans les pays du monde islamique, les données personnelles sont définies d'une manière similaire à celle de l'Union Européenne ou des pays occidentaux, en étant des données personnelles ou des informations liées à une personne physique identifiée ou identifiable. Cependant, les détails précis peuvent varier en fonction des lois spécifiques de chaque pays.

En conclusion, l'ensemble des définitions varient légèrement d'une juridiction à l'autre, mais elles partagent toutes l'idée que les données personnelles sont des informations qui permettent d'identifier ou de se relier une personne spécifique.

B. FONDAMENTAUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Le Sommet mondial sur la société de l'information (SMSI) qui s'est tenu en Tunisie en novembre 2005, a abordé la question de la protection des données dans ses documents et déclarations. La déclaration de principes de Genève adoptée lors de la première phase du SMSI en 2003, souligne la nécessité de construire la confiance et la sécurité dans l'utilisation des TICS, en favorisant la protection des données personnelles et de la vie privée ainsi que la sécurité des transactions. Cela est essentiel pour garantir l'utilisation sûre et fiable des technologies de l'information et de la communication.

Ce texte souligne l'importance de la protection des données personnelles et de la vie privée dans le contexte de l'utilisation des technologies de l'information et de la communication (TIC). La déclaration met en avant la nécessité de créer un environnement de confiance et de sécurité pour les utilisateurs.

Les fondements de la protection des données personnelles reposent sur plusieurs principes essentiels, regroupés principalement en six grands principes [5] . Ceux-ci comprennent le consentement et la transparence, la définition des finalités, la garantie de la fiabilité des données, la mise en place de mesures de sécurité et de confidentialité, ainsi que la reconnaissance et l'exercice des droits relatifs aux données.

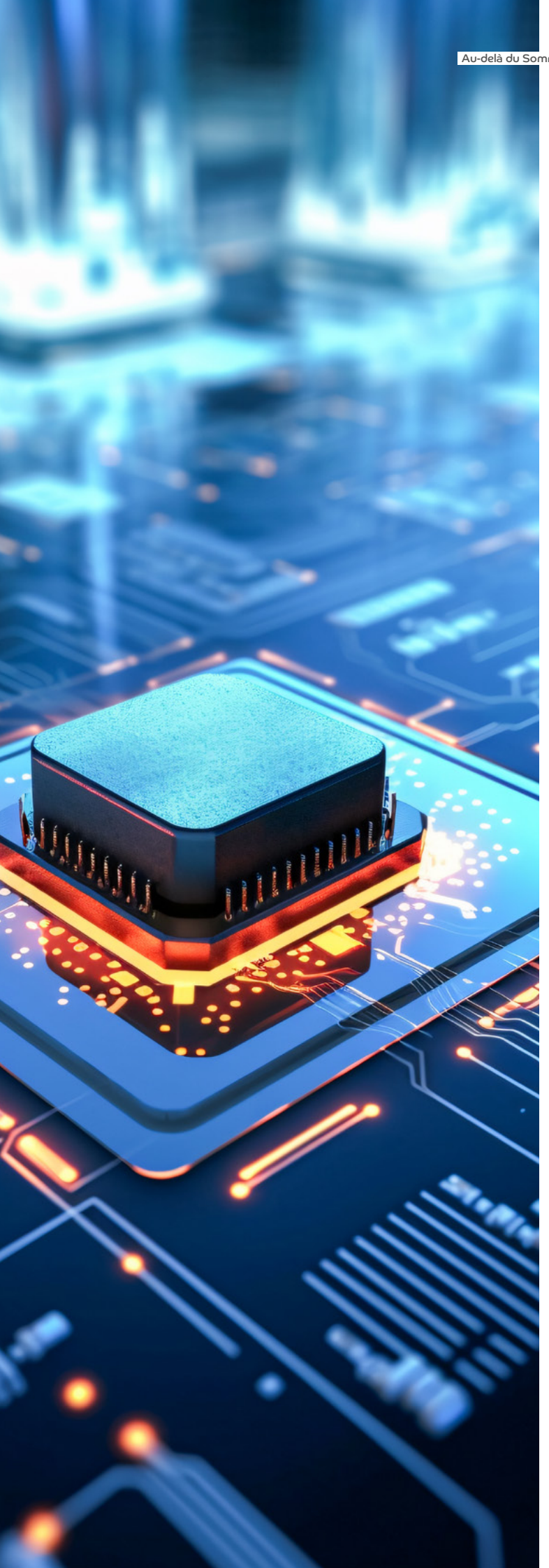
Consentement et transparence: les individus doivent donner leur consentement clair et explicite pour que leurs données personnelles soient collectées, traitées ou partagées, ainsi les organisations, ou toute personne morale ou physique, sont tenues d'être transparentes sur la manière dont elles utilisent les données personnelles et doivent aussi fournir les informations claires et compréhensibles sur l'objet, collecte, traitement et confidentialité des données personnelles.

Finalité de collecte et de traitement : les données personnelles ne doivent être collectées et traitées que dans un but spécifique et légitime, et elles ne doivent pas être utilisées ultérieurement d'une manière incompatible avec ces finalités initiales. Ainsi les organisations sont tenues de limiter la collecte des données au minimum nécessaire pour atteindre les objectifs spécifiés. Cela implique de ne collecter que les données pertinentes et proportionnées par rapport aux finalités du traitement.

Exactitude des données : Les organisations sont responsables de s'assurer que les données personnelles qu'elles détiennent sont exactes, complètes et mises à jour.

Sécurité et confidentialité : Les organisations collectant et traitant les données personnelles ont la responsabilité de mettre en place toutes les mesures de sécurité appropriées pour protéger les données personnelles contre la perte, l'accès non autorisé, la divulgation ou la destruction. Cela inclut des pratiques

[5] CNIL, le 23 août 2019, les six grands principes du Règlement Général sur la Protection des Données (RGPD), adopté le 24 mai 2016 par le Parlement européen et le Conseil. DPA: Data Protection Act 2018, https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd



telles que le cryptage des données ou la gestion des accès aux bases de données.

Respect des droits des individus : Les individus jouissent de certains droits relatifs à leurs données personnelles, notamment le droit d'accéder à leurs données, de les corriger si celles-ci sont inexactes, de les supprimer, de s'opposer à leur traitement, ou de demander leur portabilité vers un autre fournisseur de service.

Ainsi, en respectant ces principes fondamentaux, les organisations peuvent assurer une protection adéquate des données personnelles et respecter les droits et les attentes des individus en matière de vie privée.

Le respect des principes de protection des données personnelles fait partie des missions du responsable de traitement, qui peut être une entité ou une personne physique, qui détermine les finalités et les moyens du traitement des données. Il veille à ce que le traitement des données soit effectué conformément aux lois et réglementations en vigueur. Le responsable de traitement peut être une entreprise, une organisation publique ou toute autre entité qui collecte, utilise ou stocke des données personnelles. Il a la responsabilité de garantir la sécurité et la confidentialité des données, ainsi que le respect des droits des individus en matière de protection des données. En cas de non-conformité, le responsable de traitement peut être soumis à des sanctions et des amendes.

On ne peut passer sous silence, l'intelligence artificielle (IA) qui a révolutionné les pratiques de collecte, de traitement et d'utilisation des données personnelles. Grâce à l'IA, les entreprises peuvent automatiser et optimiser ces processus, offrant ainsi une personnalisation accrue des services et une analyse de données plus sophistiquée. Cependant, cela soulève également des préoccupations quant à la vie privée et à la sécurité des données, nécessitant une réglementation et une supervision appropriées.

C. ÉVOLUTION DES PRATIQUES DE COLLECTE, DE TRAITEMENT ET D'UTILISATION DES DONNÉES PERSONNELLES

Depuis les années 2000, qui étaient les années du lancement des réseaux sociaux, les pratiques de collecte, de traitement et d'utilisation des données personnelles ont radicalement évolué avec l'essor des technologies numériques. La collecte des données était pour effectuer des transactions simples, dans le domaine du commerce, il s'agissait d'enregistrement des clients pour des raisons de livraison des achats, d'envoie des factures... Ce qui constituait cette simple collecte de données pour des transactions spécifiques s'est transformé, vers l'année 2010, en un processus beaucoup plus complexe. Aujourd'hui, les données sont collectées à partir de multiples sources, y compris les réseaux sociaux, les objets connectés et les applications mobiles, capturant des informations sur les habitudes, préférences et comportements des personnes.

Le traitement de ces données s'appuie désormais sur des technologies avancées telles que le Big Data et l'intelligence artificielle. Le Big Data permet d'analyser d'énormes volumes de données en temps réel, offrant des insights précieux pour la prise de décision et la personnalisation des services. L'intelligence artificielle, quant à elle, facilite des tâches complexes comme la reconnaissance de motifs, la prédiction des comportements et l'adaptation des offres aux besoins des utilisateurs.

Cependant, cette avancée technologique pose des défis majeurs pour la protection de la vie privée. L'expansion de la collecte et de l'analyse des données accroît les risques de surveillance, de profilage et d'utilisation abusive des informations personnelles. De là, intervient le rôle de l'éducation numérique dans la sensibilisation des individus à la gestion de leurs données afin de limiter ces risques. Dans cette perspective, il y a nécessité d'établir des régulations plus strictes dans l'objectif d'encadrer l'utilisation des données et assurer une approche éthique et sécurisée, protégeant ainsi la vie privée des utilisateurs.

D. ENJEUX DE LA PROTECTION DES DONNÉES PERSONNELLES RISQUES ET CONFIANCE NUMÉRIQUE

L'instauration d'un environnement numérique plus sûr pour les interactions en ligne, qui favorise la protection des données personnelles et la confidentialité des individus et des organisations, constitue l'objectif du concept de confiance numérique. Ce concept englobe la sécurité, la confidentialité et l'intégrité des données dans le monde numérique. D'un point de vue juridique, la confiance numérique est définie par les règles et normes qui assurent cette protection, incluant la législation sur la protection des données et l'ensemble des mesures et normes de cybersécurité [6], [7].

En effet, lorsque les individus fournissent leurs informations personnelles en ligne, ils s'attendent à ce que celles-ci soient traitées de manière sécurisée et confidentielle conformément à la finalité pour laquelle elles sont collectées à la base de leur consentement préalable. Cependant, les risques de violation de la vie privée et de sécurité des données peuvent compromettre cette confiance.

Face à la cybercriminalité, aux cyberattaques, les violations de données et les pratiques de collecte et de traitement abusives peuvent entraîner des conséquences néfastes pour les individus, allant de l'usurpation d'identité, à la divulgation des données sensibles ou la fuite des données. Ces incidents voire délits portent non seulement atteinte à la vie privée des utilisateurs, mais sapent également la confiance dans les entreprises et les institutions chargées de protéger ces données.

La promotion de la confiance numérique, exige ainsi, la mise en place des mesures efficaces de protection des données [8], telles que les technologies de chiffrement et la gestion des autorisations d'accès aux bases données, et surtout la sensibilisation des utilisateurs aux bonnes pratiques en matière de cybersécurité et de protection de leurs données personnelles.

La sécurité et la confidentialité des données personnelles, constitue une composante essentielle pour renforcer la confiance des individus dans l'écosystème numérique et à favoriser un environnement en ligne plus sûr.

[6] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (France)

[7] Loi LPRPDE sur la protection des renseignements personnels et les documents électroniques (Canada)

[8] Loi n° 43-20 relative aux services de confiance pour les transactions électronique (Maroc)

2

“RENFORCEMENT INSTITUTIONNEL ET ORGANISATIONNEL RELATIF À LA PROTECTION DES DONNÉES PERSONNELLES”

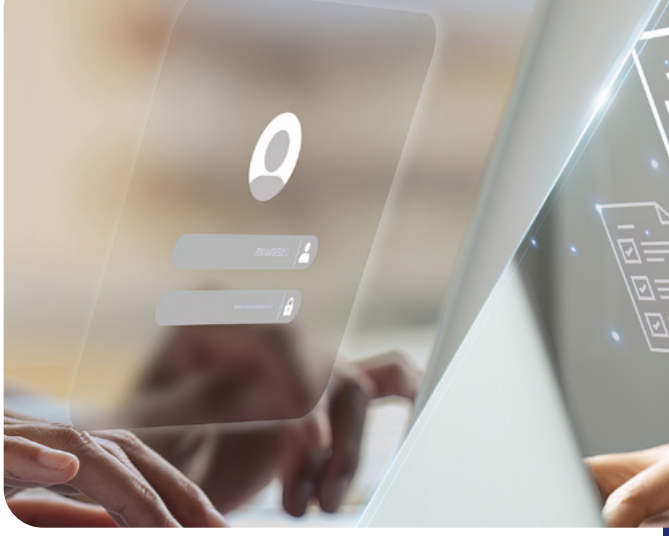
A. RÔLE ET MISSION DE L’AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLE

B. POLITIQUES INTERNES DE CONFORMITÉ AUX NORMES LÉGALES POUR UNE ORGANISATION DONNÉE

C. FORMATION SUR LES BONNES PRATIQUES DU PERSONNEL CHARGÉ DU TRAITEMENT ET DE LA GESTION DES DONNÉES PERSONNELLES

D. ADOPTION DE TECHNOLOGIES SÉCURISÉES POUR LE TRAITEMENT DES DONNÉES PERSONNELLES


AI
10 1001 01010
0 11 0010



A. RÔLE ET MISSION DE L'AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLE

L'autorité de protection des données personnelles est une entité gouvernementale indépendante chargée de veiller à la protection des données personnelles au sein du pays ou d'une région. Son rôle principal est de garantir le respect des lois et réglementations relatives à la protection des données en surveillant et en régulant les activités de traitement des données. Elle agit en tant qu'organe de contrôle ou de surveillance de l'application des lois relatives à la protection des données personnelles et la mise en conformité. Elle est également chargée de mener des enquêtes sur les éventuelles violations présumées, et peut imposer des sanctions en cas de non-conformité. De plus, elle fournit, accompagne et oriente les entreprises et les individus sur les bonnes pratiques en matière de protection des données. Elle joue également un rôle de sensibilisation du grand public sur les enjeux de la protection de la vie privée et de la sécurité des données.

En outre, dans le contexte d'un monde numérique connecté, l'autorité de protection des données personnelles est appelée à collaborer avec les autorités nationales en charge de la sécurité et de la cybersécurité, mais également avec d'autres autorités de protection des données à l'échelle internationale dans le but de promouvoir la coopération et l'harmonisation des normes de protection des données.

B. POLITIQUES INTERNES DE CONFORMITÉ AUX NORMES LÉGALES POUR UNE ORGANISATION DONNÉE

Quant il s'agit d'un organisme structuré, comme une entreprise par exemple, il est crucial d'adopter des politiques internes de conformité aux normes légales et aux réglementations de protection des données personnelles, afin de garantir l'adhésion de cette structure aux principes la confiance numérique et le respect de la vie privée. Une telle politique inclue des procédures claires et des lignes directrices qui guident les différents cycles de la protection des données, à savoir la collecte, le traitement et le stockage, en veillant à ce qu'elles soient conformes aux lois et réglementations en vigueur. Pour se faire il essentiel de nommer un responsable de la protection des données (Data Protection Officer DPO, en anglais), chargé de surveiller et de superviser la conformité aux normes de protection des données..

Dans tous les États membres de l'Union européenne (UE), conformément au Règlement général sur la protection des données (RGPD), toutes les entreprises qui manipulent des données personnelles sont tenues de nommer un délégué à la protection des données (DPO).

Afin d'être en parfaite conformité aux normes légales de protection des données personnelles et de s'adapter à l'évolution technologique et juridique, toute organisation qui traite les données personnelles est sensé d'établir des programmes de formation continue. Ces programmes visent à renforcer les compétences des responsables et à sensibiliser le personnel aux bonnes pratiques en matière de protection des données ainsi qu'aux risques associés à la violation de la vie privée.

C. FORMATION SUR LES BONNES PRATIQUES DU PERSONNEL CHARGÉ DU TRAITEMENT ET DE LA GESTION DES DONNÉES PERSONNELLES

Le renforcement de capacités de l'organisation en matière de protection des données personnelle nécessite la mise en place d'un programme de formation sur les bonnes pratiques destinées au personnel chargé du traitement et de la gestion des données personnelles, ainsi qu'à l'ensemble du personnel. Ceci suppose l'identification en amont des besoins spécifiques en formation en fonction des rôles et responsabilités de l'ensemble du personnel concerné.

Le programme de formation à mettre en place doit être bien élaboré, dans la mesure ou il devra contenir des supports qui mettent en lumière les principes et les fondements de la protection des données, les obligations légales et réglementaires, les risques liés à la violation de la vie privée et les mesures de sécurité à adopter, afin de garantir l'adhésion du personnel aux objectifs de la formation, le programme devrait être interactif et inclusif, impliquant des ateliers pratiques et des études de cas. De plus, il est important de faire appel à des formateurs qualifiés ou des experts en la matière, en se basant sur des ressources et des outils andragogiques adéquats. Il est également essentiel de tenir des sessions de sensibilisation régulières pour rappeler les bonnes pratiques et les obligations en matière de protection des données.

Il est également opportun de mettre en place un mécanisme pour mesurer l'efficacité du programme de formation à l'aide des évaluations permanentes, et procéder à des ajustements du contenu et les approches pédagogiques ou andragogiques en fonction des retours d'expérience pour assurer une formation continue, permetant aux bénéficiaires, ainsi qu'à l'organisation d'être en conformité optimale avec les normes de protection des données.

Par exemple, pour sensibiliser et accompagner les entreprises dans leur conformité au Règlement Général sur la Protection des Données (RGPD), la CNIL en France a créé un programme de formation en ligne. Principalement destiné aux actuels et futurs délégués à la protection des données (DPO) ainsi qu'aux professionnels souhaitant se familiariser avec le RGPD, ce programme consiste en des ateliers de formation sous forme de Mooc accessibles à tous. Ces ateliers comprennent des vidéos, des textes, des illustrations et des cas pratiques, ainsi que des quiz et des évaluations. Les quatre principaux modules abordent les concepts clés du RGPD, à savoir :

Module 1 : le RGPD et ses notions clés

Module 2 : les principes de la protection des données

Module 3: les responsabilités des acteurs

Module 4 : le DPO et les outils de la conformité

La formation est gratuite et ouverte à tous, et à la fin de chaque module, une attestation est délivrée aux participants ayant suivi la formation.

[9] Ateliers de formation RGPD(MOOC) de la CNIL (France)
https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

D. ADOPTION DE TECHNOLOGIES SÉCURISÉES POUR LE TRAITEMENT DES DONNÉES PERSONNELLES

Le traitement des données personnelles, en particulier celles considérées comme sensibles, requiert une approche spécifique pour garantir leur sécurité. Il est essentiel d'adopter des systèmes techniques de protection robustes, notamment en utilisant des technologies de chiffrement fondées sur des algorithmes de cryptographie solides.

A titre d'exemple

AES (Advanced Encryption Standard) : qui est l'un des algorithmes de chiffrement symétrique les plus utilisés, approuvé par le gouvernement américain pour protéger les informations sensibles.

RSA (Rivest-Shamir-Adleman) : Il s'agit d'un algorithme de chiffrement asymétrique largement utilisé pour la sécurité des communications sur Internet. RSA utilise une paire de clés (publique et privée) pour chiffrer et déchiffrer les données, offrant ainsi une sécurité robuste pour les données personnelles.

ECC (Elliptic Curve Cryptography) : algorithme de chiffrement asymétrique, bien adapté à la protection des données personnelles sur les appareils mobiles et les systèmes embarqués.

Ces technologies de chiffrement, et bien d'autres, sont essentielles pour protéger les données personnelles lors de leur traitement, aussi dans leur transmission et de leur stockage. De plus, l'utilisation de pare-feu et de logiciels antivirus peut aider à prévenir les cyberattaques et les violations de sécurité.

Le renforcement de la sécurité peut également recourir à des solutions d'authentification multi-facteurs en exigeant plusieurs formes d'identification avant d'accéder aux données. De plus, les outils de gestion des identités et des accès permettent de contrôler et de limiter l'accès aux données en fonction des rôles et des permissions des utilisateurs.

3

“EDUCATION NUMÉRIQUE ET PROTECTION DES DONNÉES PERSONNELLES”

A. EDUCATION NUMÉRIQUE ET DONNÉES PERSONNELLES

B. MISE EN PLACE DE PROGRAMMES ÉDUCATIFS ET DE COMMUNICATION

C. BONNES PRATIQUES POUR UN USAGE SÉCURISÉ DES TECHNOLOGIES NUMÉRIQUES.

D. SENSIBILISATION ET RESPONSABILITÉ INDIVIDUELLE ET COLLECTIVE

A. EDUCATION NUMÉRIQUE ET DONNÉES PERSONNELLES

L'éducation numérique et la protection des données personnelles sont étroitement liées. En effet, l'éducation numérique permet de sensibiliser les jeunes utilisateurs certes, mais également les seniors, aux enjeux de la protection des données personnelles, en les aidant à comprendre les multiples risques liés à la divulgation d'informations personnelles en ligne et en leur fournissant les connaissances nécessaires pour se prémunir des dangers.

De plus, une éducation numérique solide permet aux individus de développer les compétences nécessaires pour protéger leurs données personnelles, en apprenant les bonnes et meilleures pratiques de confidentialité et de protection de la vie privée sur les plateformes en ligne, à reconnaître les diverses facettes de cybercriminalité ainsi que ses vecteurs d'attaque tels que le phishing, l'usurpation d'identité, etc. Cette compréhension approfondie des risques en ligne aidera les personnes à adopter des pratiques de sécurité des données appropriées.

L'éducation numérique dès le plus jeune âge, suppose l'intégration des concepts et bonnes pratiques de la protection des données personnelles dans les programmes d'éducation, contribue à promouvoir la culture de la confidentialité et de la sécurité des données, essentiel pour prévenir les violations de la vie privée la renforcent la confiance dans l'environnement numérique.

En outre, une éducation numérique efficace peut également jouer un rôle essentiel dans la sensibilisation aux droits des individus en matière de protection des données et à la responsabilité des responsables des traitement des données chez les organisations et les entreprises, contribuant ainsi à promouvoir l'usage éthique et responsable de la technologie.

Finalement, l'éducation numérique et la protection des données personnelles sont complémentaires et se renforcent mutuellement pour favoriser un environnement numérique plus sûr, sécurisé et respectueux de la vie privée.

B. MISE EN PLACE DE PROGRAMMES ÉDUCATIFS ET DE COMMUNICATION

La mise en place de programmes éducatifs et de communication, tels que l'Education aux Média et à l'Information (EMI) portant sur la protection des données personnelles est de grande importance dans l'instauration de la culture numérique et le renforcement de la compréhension des individus des risques potentiels liés à la divulgation d'informations personnelles en ligne et hors ligne. Ce type de programme développe une compréhension de leurs droits, de leurs responsabilités et de l'importance de la protection de leur vie privée. Ces programmes seront donc conçus pour informer, sensibiliser et éduquer les individus sur l'importance de protéger leurs données personnelles et sur les bonnes pratiques à adopter pour assurer leur sécurité en ligne. Ils peuvent prendre diverses formes, dépendamment du contexte et de la cible. Ils peuvent être organisés sous forme de séminaires interactifs, d'ateliers pratiques, de campagnes de sensibilisation en ligne ou hors ligne, de cours ou des supports pédagogiques.

À l'heure actuelle, les pays scandinaves, célèbres pour l'excellence de leurs systèmes éducatifs, intègrent des programmes visant à sensibiliser à la protection des données personnelles. Voici quelques caractéristiques spécifiques de ces modèles scandinaves. À titre d'exemple, la Norvège a mis en place des politiques éducatives visant à former des citoyens conscients et informés de la protection de leurs données personnelles.

En Norvège, les élèves sont initiés aux principes de la confidentialité en ligne, aux risques associés à la divulgation d'informations personnelles et aux bonnes pratiques pour protéger leur vie privée. Ils sont également sensibilisés à leurs droits en tant qu'utilisateurs d'Internet, apprenant à gérer leurs paramètres de confidentialité sur les plateformes en ligne, à interpréter les conditions d'utilisation et à exercer leurs droits sur leurs données personnelles. Les enseignants norvégiens reçoivent une formation sur la sensibilisation à la protection des données, leur permettant ainsi de transmettre ces connaissances à leurs élèves et de les guider vers une utilisation responsable d'Internet. De plus, les écoles encouragent l'implication des parents dans l'éducation à la protection des données.

À cet effet, des ateliers et des sessions d'information sont organisés pour les parents afin de les aider à saisir les enjeux liés à la vie privée en ligne.

Il est essentiel que les programmes éducatifs soient adaptés à l'âge et aux besoins, en fournissant des conseils pratiques, simples et claires sur la manière de protéger efficacement les données personnelles. Il est par ailleurs important de mettre l'accent sur les aspects techniques et juridiques pour développer les compétences des apprenants dans la gestion des paramètres de confidentialité sur les réseaux sociaux, la sécurisation des mots de passe et la reconnaissance des tentatives de phishing, la protection contre les logiciels malveillants, ainsi que la connaissance des réglementations et lois relatives à la protection des données personnelles, en expliquant les différents droits, tel que le consentement, le droit d'accès aux informations personnelles collectées ou le droit d'opposition ou de rectification.

Enfin, adopter une communication efficace et appropriée joue un rôle crucial dans la diffusion de la culture numérique, une culture articulée autour des droits à la vie privée et de protection des données personnelles, encourageant ainsi une prise de conscience collective et une adoption de comportements responsables dans l'utilisation de la technologie.

C. BONNES PRATIQUES POUR UN USAGE SÉCURISÉ DES TECHNOLOGIES NUMÉRIQUES.

Pour une meilleure protection des données personnelles dans l'environnement numérique, il est essentiel que les usagers des nouvelles technologies, développent un comportement vigilant en ligne. Les différentes formations permettront aux usagers d'adopter le comportement responsable idéal basé sur le respect d'une liste non exhaustive des bonnes pratiques de base de cybersécurité, telles que :

- Usage des mots de passe forts et uniques pour chaque compte en ligne, des mots de passes sous forme de combinaison de lettres, de chiffres et de caractères spéciaux,
- Activation de l'authentification à deux facteurs lorsque cela est possible, cela permet d'ajouter une couche de sécurité supplémentaire aux comptes sur les réseaux sociaux, les boites mails ou les jeux en ligne par exemple,
- Réduction aux maximum possible les informations personnelles partagées en ligne, en ne les partagean que si c'est nécessaire, en s'assurant tout d'abord que les sites de navigation sont des sites de confiances et sécurisés, et en ajustant les paramètres de confidentialité sur les plateformes en ligne,
- Installation de logiciel antivirus et de pare-feu pour protéger les appareils contre les logiciels malveillants, l'espionnage, et les menaces en ligne,
- Mise à jour régulière des logiciels, applications et systèmes d'exploitation afin de bénéficier des derniers correctifs de sécurité, permettant de faire face aux vulnérabilités potentielles
- Être méfiant des liens non sécurisés ou des pièces jointes provenant de sources non fiables ou inconnues, pour se protéger contre les attaques de phishing qui sont conçues spécialement pour vol des données personnelles ou sensibles,
- Être méfiant des connexions à des réseaux Wi-Fi publics non sécurisés, surtout lorsqu'il s'agit de transactions sensibles ou d'accès à des comptes personnels.

- Être vigilant face aux tentatives de fraude ou d'usurpation d'identité en vérifiant l'authenticité des communications et en signalant tout comportement suspect.
- Cependant, la rapide progression des technologies numériques a entraîné une augmentation significative des risques, notamment avec la multiplication des objets connectés, la généralisation de l'intelligence artificielle, et l'avènement du metavers. Dans ce contexte, il est impératif d'accroître notre vigilance pour assurer une navigation sécurisée. Cela nécessite l'adoption de plus de pratiques adaptées, comme :
- Se renseigner sur les objets connectés (Smart montre, domotique, caméra, etc.), et s' informer sur ses caractéristiques, son fonctionnement et ses interactions avec d'autres appareils électroniques. Les objets connectés présentent encore des failles de sécurité en termes de protection des données personnelles;
- Protéger les données personnelles surtout sensibles, utilisées par les systèmes d'Intelligence Artificielle, en mettant en œuvre des mesures de sécurité robustes, telles que le chiffrement, la pseudonymisation et la gestion des accès. Il est crucial de veiller à ce que les données sensibles traitées par l'IA soient sécurisées et conforme aux réglementations en vigueur.
- Mettre en place des mécanismes de surveillance continue pour détecter les anomalies et les dérives dans le comportement des systèmes d'IA en production, et réagir rapidement aux problèmes identifiés pour prévenir les conséquences néfastes.
- Rester vigilant face aux nouvelles techniques de phishing alimentées par l'intelligence artificielle, qui cherchent à dérober les données personnelles. Ces attaques sophistiquées peuvent utiliser des algorithmes d'IA pour personnaliser les messages et contourner les défenses traditionnelles.

D. SENSIBILISATION ET RESPONSABILITÉ INDIVIDUELLE ET COLLECTIVE.

La sensibilisation à la protection des données personnelles dans l'environnement numérique est essentielle où les informations personnelles sont de plus en plus vulnérables aux menaces en ligne, surtout avec l'évolution des technologies numériques, à savoir en particulier les applications des technologies de l'intelligence artificielle. La sensibilisation permet aux individus de bien comprendre les enjeux et les risques potentiels liés à la divulgation d'informations ou données personnelles en ligne. La sensibilisation les encourage également à reconnaître l'importance de préserver la vie privée dans leur quotidien, mais aussi pour encourager l'émergence d'une société de l'information et de la connaissance basée sur la confiance numérique.

En revanche, la protection des données personnelles dans l'environnement numérique, est une responsabilité partagée entre l'individu concerné et les différentes parties prenantes. C'est également une affaire collective da la société. En d'autres termes, cette responsabilité implique que chaque personne prend des mesures pour protéger ses propres données personnelles, en adoptant des bonnes pratiques de sécurité en ligne, tout en étant conscient du volet juridique et réglementaire. Quant à la responsabilité collective, elle incombe à la société dans son ensemble. Il faudra également travailler de manière collective pour promouvoir une culture de la protection des données personnelles, en mettant l'accent sur la sensibilisation et l'éducation de l'ensemble des citoyens aux droits à l'image dans les plateformes numériques et sur les réseaux sociaux. Ce volet est essentiel et doit impliquer l'ensemble de la communauté éducative comme les parents, les tuteurs et les enseignants qui ont tous un rôle crucial à jouer dans cette démarche.

[10] Loi n° 2024-120 du 19 février 2024 (France)

4

“PROTECTION DES DONNÉES PERSONNELLES DANS LES ETATS MEMBRES DE L’ICESCO”

A. RÉGLEMENTATIONS NATIONALES ET INTERNATIONALES EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

B. ANALYSE COMPARATIVE DES LÉGISLATIONS NATIONALES DES PAYS MEMBRES DE L’ICESCO

C. DÉFIS LIÉS À L’HARMONISATION DES RÉGLEMENTATIONS ET DES PRATIQUES

D. DÉFIS DE MIS EN PLACE DE STRATÉGIE DE SENSIBILISATION ET DE RENFORCEMENT DE CAPACITÉS.


Card Purchased
Wallet Recharge
Search
Finance business

A. RÉGLEMENTATIONS NATIONALES ET INTERNATIONALES EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

Les réglementations nationales et internationales en matière de protection des données personnelles jouent un rôle crucial dans la préservation de la vie privée et de la sécurité des individus. Les premières préoccupations internationales concernant la protection des données et de la vie privée qui ont inspiré des règlementations récentes face aux avancées technologiques remontent aux années 1970.

Au fil des décennies, plusieurs étapes clés ont été franchies, notamment l'adoption de lois telles que le Privacy Act aux États-Unis dans les années 1980 et la Convention 108 du Conseil de l'Europe en 1981, ainsi que l'adoption de réglementations plus récentes telles que le RGPD de l'Union européenne en 2016. Ces réglementations visent à protéger les droits fondamentaux des individus dans un monde numérique.

Diverses organisations internationales telles que les Nations Unies, l'Organisation de Coopération et de Développement Économiques (OCDE) ou le Conseil de l'Europe et, ont élaboré des instruments et des recommandations visant à promouvoir une protection uniforme des données personnelles à l'échelle mondiale. Parmi les textes les plus importants figurent la Déclaration universelle des droits de l'homme (1948), Convention 108 du Conseil de l'Europe (1981), Directive de l'Union Européenne sur la protection des données (1995) et Règlement général sur la protection des données (RGPD) (2018) .

Au niveau national, de nombreux pays ont adopté des lois spécifiques sur la protection des données, telles que la Loi sur la Protection des Données Personnelles (PDPL) en Corée du Sud ou encore la California Consumer Privacy Act (CCPA) aux États-Unis. Ces lois établissent des normes et des exigences strictes en matière de collecte, de traitement et de stockage des données personnelles, ainsi que des mécanismes pour faire respecter ces règles et sanctionner les violations.

Ces réglementations nationales et internationales établissent un cadre juridique garantissant que les données personnelles sont traitées de manière éthique, sécurisée et conforme aux droits fondamentaux des individus. Elles encouragent également la coopération entre les pays pour relever les défis transfrontaliers liés à la protection des données, tels que le transfert international de données et la lutte contre la cybercriminalité. En favorisant une approche harmonisée de la protection des données à l'échelle mondiale, ces réglementations contribuent à renforcer la confiance au numérique des individus et à promouvoir le respect de la vie privée comme étant un droit fondamental.

B. ANALYSE COMPARATIVE DES LÉGISLATIONS NATIONALES DES PAYS MEMBRES DE L'ICESCO

Parmi les Etats membres de l'ICESCO, certains ont déjà développé des approches variées en matière de protection des données personnelles, influencées par des facteurs culturels, politiques et juridiques propres à chaque Etat. La plupart des Etats membres ont mis en place des lois de protection des données plus avancées et rigoureuses, tandis que d'autres disposent de cadres réglementaires en cours de réflexion.

L'analyse comparative fourni dans le présent guide, permet une première lecture des avancées et une compréhension des similitudes et des différences entre les législations nationales concernant la définition des données personnelles, les droits des individus, les responsabilités des organisations, les mécanismes de surveillance et les sanctions en cas de non-conformité.

A titre exemple, certains pays accordent une importance particulière à la protection des données sensibles, telles que les données biométriques ou médicales, tandis que d'autres mettent l'accent sur la protection des données financières ou commerciales.

De plus, cette analyse pourrait explorer comment les Etats membres de l'ICESCO répondent aux nouveaux défis en matière de protection des données, tels que la régulation de l'intelligence artificielle et de l'Internet. Elle pourrait également examiner les préoccupations du moment, comme la gestion des données biométriques, la protection contre les cyberattaques et la transparence des algorithmes, révélant ainsi les stratégies adoptées pour assurer la sécurité et la confidentialité dans le paysage numérique.

Une vue d'ensemble du cadre juridique et réglementaire concernant la protection des données au sein de l'ensemble des États membres de l'ICESCO révéle une diversité de stratégies et d'approches. Elle souligne l'importance de la coopération inter-régionale et internationale pour relever les défis communs dans ce domaine.

Une analyse comparative exhaustive des lois sur la protection des données adoptées par les pays membres de l'ICESCO est indispensable pour identifier les divergences éventuelles. Ces divergences peuvent représenter un défi pour la collaboration et la cohérence entre les différents cadres réglementaires nationaux. En établissant des normes communes, les pays membres pourraient travailler ensemble pour relever les défis partagés liés à la protection des données dans un environnement numérique mondialisé.

Le tableau récapitulatif de ce guide offre un aperçu du paysage des législations nationales relatives à la protection des données personnelles dans certains Etats membres de l'ICESCO.

	Pays membre	Références juridiques	Autorité responsable
1	Royaume du Maroc	Loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	Commission Nationale de Contrôle de Protection des données à Caractère Personnel (CNDP)
2	République Islamique De Mauritanie	Loi n° 2017-020 du 22 juillet 2017 relative à la protection des données à caractère personnel	Autorité de Protection des Données à Caractère Personnel (APDCP)
3	République du Niger	Loi n° 2023-31 du 04 juillet 2023 modifiant la loi n°2022-59 du 16 décembre 2022 relative à la protection des données personnelles et la loi n°2022-59 du 16 décembre 2022 relative à la protection des données personnelles	Haute Autorité pour la Protection des Données Personnelles (HAPDP)
4	République Fédérale Du Nigeria	Loi promulguée en 2023 « Nigeria Data Protection Act »	Comission Nigériane de protetion des données (NDPC)
5	République Du Yemen	Néant	Néant
6	République Du Bénin	Le régime de protection des données au Bénin est régi par deux textes législatifs à savoir la loi n° 2017-20 du 20 avril 2018 portant code numérique et la loi n° 2009-09 du 22 mai 2009 relative à la protection des données personnelles.	Autorité béninoise de protection des données
7	République De Côte D'ivoire	Loi 2013-450 relative à la protection des données personnelles	Autorité de Régulation des Télécommunications TIC de Côte d'Ivoire
8	Koweït	Décision n° 42 de 2021 sur le règlement sur la protection de la confidentialité des données	Autorité de régulation des communications et de télécommunications «CITRA»

9	Liban	Loi n°81-2018	Ministère de l'Économie et du Commerce
10	Libye	La Constitution de 2011. Articles 12 et 13	Néant
11	République Du Maldive	Aucune loi spécifique	Néant
12	République Du Mali	Loi n° 2013-015	Autorité de protection des données à caractère personnel
13	La Malaisie	Loi sur la protection des données personnelles de 2010 (PDPA)	La Direction de la Protection des Données Personnelles
14	L'Egypte	Loi n° 151 de 2020 sur la protection des données personnelles	Autorité nationale de protection des données personnelles.
15	République De La Guinée	loi 37/2016 relative à la cybersécurité et la protection des données à caractère Personnel.	Autorité chargée de la cybersécurité ANSSI
16	Palestine	Néant	Néant
17	République Du Kazakhstan	Loi n° 94-V du 21 mai 2013	Ministère du Développement Numérique, de l'Innovation et de l'Industrie aérospatiale
18	Quatar	Loi n°.13 de 2016 relative à la protection des données personnelles.	National Cyber Governance and Assurance Affairs(NCGAA)
19	Union Des Comores	Néant	Néant
20	République Kirghize	Loi n° 58 du 14 avril 2008	Agence d'État pour la protection des données personnelles.

21	République du Cameroun	Loi n° 2010/013 du 21/12/ 2010 modifiée et complétée par la loi N°2015/06 du 20 avril 2015 régissant les communications électroniques au Cameroun	Autorité de Régulation des Télécommunications
22	République De Sierra Leone	Néant	Néant
23	Sénégal	Loi n° 2008-12 du 25 janvier 2008	Commission de Protection des Données Personnelles
24	République Fédérale De Somalie	Loi n° 005 de 2023	Data Protection Authority
25	République D'Irak	Néant	Néant
26	Sultanat D'Oman	Arrêté royal n°6 de 2022	Néant
27	République Gabonaise	Acte n° 025/2023 du 09/07/2023 modifiant la loi n° 001/2011 du 25 septembre 2011	Autorité de protection des données personnelles et de la vie privée APDPVP
28	République De Gambie	Projet de loi en cours	Néant
29	République De Guyana	La loi n° 18 de 2023 sur la protection des données personnelles	Data protection Commissioner
30	Tunisie	Loi n° 2019-014 du 29 octobre 2019	Instance de Protection des Données à Caractère Personnel (IPDCP)
31	Algérie	Loiorganique n°63469–2004, décret n°3003470–2007	Instance Nationale de Protection des Données à Caractère Personnel (INPDP)
32	République De Djibouti	Projet de loi	Néant

33	Arabie Saoudite	Décret royal n° M/19 du 9/2/1443H (correspondant au 16 septembre 2021), telle que modifiée par le décret royal n° M/148 du 5/9/1444H (correspondant au 27 mars 2023)	Autorité Saoudienne pour les Données et l'Intelligence Artificielle (« SDAIA »)
34	Sudan	Néant	Néant
35	République Du Suriname	Projet de loi	Néant
36	Syrie	Néant	Néant
37	Pakistan	Projet de loi	Néant
38	Bahreïn	Loi n° 30 de 2018, entrée en vigueur le 1er août 2019 « PDPL »	Ministère de la Justice, des Affaires Islamiques et des Dotations
39	Brunéi Darussalam	Projet de loi 2021 sur la protection des données personnelles	Autorité pour l'industrie de technologie de l'information et des communications
40	Bangladesh	Pas de loi spécifique Loi de 2023 sur la cybersécurité	Agence de cybersécurité
41	République Du Bénin	Loi n°2017-20, la loi n°2009-09	Autorité de Protection des Données à caractère Personnel (APDP
42	Burkina-Faso	Loi n°010-2004/AN	La Commission de l'Informatique etdes Libertés (CIL)
43	République Tadjikistan	Loi n°1537, du 3/8/2018, loi n° 631 du 15/5/2002, sur la protectiondesdonnées	Service de communication du gouvernement de la République du Tadjikistan
44	République Du Tchad	Loi n°007/PR/2015 régi la protection des données	Agence Nationale de Sécurité Informatique et de Certification Electronique
45	République Islamique D'Iran	Néant	Néant

46	Ouganda	La loi n° 9 de 2019 sur la protection des données et la vie privée	Bureau de protection des données personnelles qui relève de l'Autorité nationale des technologies de l'information
47	Jordan	Loi n°24/2023 sur la protection des donnéespersonnelles	Néant
48	République d'Ouzbékistan	Loi n°ZRU-547, sur les données personnelles	Agence de personnalisation relevant du Ministère de la Justice
49	République D'Indonésie	Projet de loi	Néant
50	Etats Des Emirates Arabes Unies	Décret-loi fédéral n°45 de 2021 sur la protection des données personnelles	Office of data protection (ODP)
51	République Islamique D'Afghanistan	Néant	Néant
52	République D'Azerbaïdjan	Loi n°998-IIIQ, du 11/05/2010 sur les données personnelles	

C. DÉFIS LIÉS À L'HARMONISATION DES RÉGLEMENTATIONS ET DES PRATIQUES

Il apparait important d'harmoniser les réglementations internationales et les bonnes pratiques en matière de protection des données personnelles, car elle favorise la cohérence entre les juridictions à l'échelle mondiale, permettant ainsi le respect des normes pour les entreprises et organisations opérant à l'international. Elle permet également de garantir des normes élevées de transparence et de sécurité des données circulant à l'échelle mondiale, en plus de faciliter la coopération internationale dans la lutte contre les menaces transfrontalières telles que la cybercriminalité.

Sur le plan pratique, l'harmonisation des réglementations est confrontée à des défis majeurs, résidant dans les différences culturelles, politiques et juridiques entre les pays, ce qui rend difficile l'élaboration de normes et de règles régionales ou universelles. En effet, chaque pays a ses propres spécificités, sa propre approche de la protection des données et son propre système juridique, ce qui rend complexe la mise en place d'une réglementation harmonisée à l'échelle internationale.

A ceci s'ajoute le contexte technologique en constante évolution et qui pose des défis supplémentaires. En effet, devant les disparités technologiques telles que l'intelligence artificielle, l'Internet des objets et la blockchain, la collecte, le traitement et la manipulation des données personnelles deviennent déséquilibrées. Ce déséquilibre impose la mise en place d'une réglementation agile et adaptable. De plus, les entreprises et les organisations opérant à l'échelle internationales sont confrontées à de multiples défis de conformité vis-à-vis des différentes lois des autres pays.

Actuellement, l'évolution des risques liés aux violations de données personnelles et l'atteinte à la vie privée, mettent en lumière la nécessité de rapprocher les réglementations des pays. C'est le cas par exemple des pays de l'Union européenne, qui ont adopté le RGPD, qui répond aux défis de diversité des réglementations, et qui facilite ainsi la libre circulation des données au sein de l'Union Européenne.

Pour contrer la série de défis cité auparavant, il devient nécessaire d'harmoniser les réglementations entre les pays et les pratiques de protection des données personnelles, non seulement pour garantir une protection adéquate des droits fondamentaux des individus dans un environnement numérique mondialisé, mais aussi pour favoriser la libre circulation des données à l'échelle mondiale, facilitant ainsi le développement international et la collaboration transfrontalière. Pour atteindre cet objectif, une coopération étroite entre les gouvernements, les organisations internationales, les entreprises et la société civile sont à favoriser pour développer des normes et des principes communs qui restaurent la confiance et la transparence dans le traitement des données personnelles, surtout pour des pays qui partagent des cultures ou des références communes.

D. DÉFIS DE MIS EN PLACE DE STRATÉGIE DE SENSIBILISATION ET DE RENFORCEMENT DE CAPACITÉS

La mise en place d'une stratégie de sensibilisation et de formation sur la protection des données personnelles est confrontée à plusieurs défis sur le plan pratique. Le défi majeur réside dans la difficulté de généralisation de la sensibilisation au sein de la population, qui peut ne pas être pleinement consciente des risques liés à la divulgation de données personnelles. De plus, il est essentiel de répondre à une diversité des besoins et des niveaux de compréhension de la population, en adaptant les programmes de sensibilisation ou de renforcement de capacités à différents publics, y compris les professionnels, les jeunes utilisateurs et les enfants. Ce qui suppose la mise en place des stratégies agiles adaptées aux spécificités de chaque public cible.

Pour faire face aux évolutions des technologies et des pratiques en matière de protection des données personnelles, une constante mise à jour des contenus et des approches pédagogiques s'impose. Toutefois, le désengagement de certains publics cibles dans les programmes de sensibilisation peut compromettre l'impact et l'efficacité des formations à long terme. De plus, la mise en place des stratégies de sensibilisation et de formation engendre un coût financier et des ressources humaines qualifiées, dont l'absence peut constituer des obstacles à la mise en œuvre de programmes de sensibilisation et de formation complets, pérennes et de qualité.

La mise en place de mécanismes d'évaluation des stratégies de sensibilisation ou de formation est une étape importante pour mesurer l'impact des programmes, évaluer son efficacité et apporter les ajustements nécessaires pour améliorer, de manière constante, la stratégie relative à la protection des données personnelles dans l'espace numérique.

5

“PROTECTION DES DONNÉES PERSONNELLES ET RENFORCEMENT DE LA COOPÉRATION ENTRE LES ETATS MEMBRES DE L’ICESCO”

A. QUELQUES MODÈLES DE MÉCANISME DE COOPÉRATION RÉUSSIS

B. DÉVELOPPEMENT DES NORMES DE BASE COMMUNES ET CONFORMITÉ

C. MÉCANISME DE COOPÉRATION ET RENFORCEMENT DE CAPACITÉS DANS LES PAYS MEMBRES DE L’ICESCO.

A. QUELQUES MODÈLES DE MÉCANISME DE COOPÉRATION RÉUSSIS

La coopération internationale pour la protection des données personnelles est essentielle pour garantir un niveau de protection uniforme et élevé à l'échelle internationale, renforçant ainsi la confiance des individus dans l'utilisation des technologies numériques. Elle facilite également l'échange d'informations et de bonnes pratiques entre les autorités chargées de la protection des données, renforçant ainsi leur capacité à répondre aux défis croissants liés à la protection des données. Elle favorise la cohérence des normes et des réglementations en matière de protection des données, ce qui réduit les obstacles au développement international et facilite le transfert transfrontalier de données tout en garantissant le respect des droits fondamentaux en matière de vie privée.

Conscients des multiples avantages d'une telle coopération internationales, plusieurs Etats ont opté pour la mise en place des instruments et de conventions internationales ou régionales.Voici quelques modèles de mécanismes de coopération réussis dans le domaine de la protection des données personnelles :

- Convention 108 et 108 plus, du Conseil de l'Europe, qui constitue le premier instrument juridiquement contraignant en matière de protection des données au niveau international. La convention fournit un cadre pour la coopération entre les États membres du Conseil de l'Europe en matière de protection des données personnelles et encourage l'adoption de normes communes de protection des données pour l'ensemble des pays hors l'Union Européenne.
- Accord de coopération en matière de protection des données personnelles entre l'UE et le Japon,

cet accord vise à faciliter le transfert de données personnelles entre l'UE et le Japon en reconnaissant les systèmes de protection des données de chaque partie comme adéquats, ce qui permet aux entreprises de transférer des données en toute sécurité sans avoir besoin de mécanismes supplémentaires de garantie.

- Groupe de travail sur la protection des données au sein de l'organisation de coopération et de développement économiques (OCDE), le groupe réunit des représentants de gouvernements et d'organisations internationales autour des défis émergents en matière de protection des données et développe des lignes directrices et des recommandations pour les politiques nationales.
- Réseaux régionaux de protection des données: il s'agit des mécanismes mis en place par quelques pays pour faciliter la coopération et l'échange d'informations entre les autorités de protection des données à l'échelle régionale.Ces réseaux fournissent un forum pour partager les meilleures pratiques, coordonner les enquêtes transfrontalières et promouvoir la convergence des normes de protection des données, il s'agit par exemple du Réseau Africain de Protection des Données Personnelles (APDPN), l'Association des Nations de l'Asie du Sud-Est (ASEAN), ou le Réseau Latino-Américain de Protection des Données Personnelles (RLDCP).

Une analyse comparative pourrait également mettre en lumière les initiatives de coopération et d'harmonisation des législations nationales entre les pays membres de l'ICESCO, visant à renforcer la protection des données personnelles à l'échelle régionale ou internationale. Cela pourrait inclure des accords de partage d'informations, des programmes d'assistance technique et des mécanismes de coopération.

B. DÉVELOPPEMENT DES NORMES DE BASE COMMUNES ET CONFORMITÉ

Avec le développement des services numériques et le flux des données entre les pays, Il s'avère primordial d'établir des normes communes et la création d'un cadre cohérent et harmonisé pour la protection des données reconnu à l'échelle internationale. Bien que le développement de normes de base communes et la conformité à la protection des données personnelles soit crucial, Il engendre également plusieurs avantages significatifs. Tout d'abord il permet de faciliter la compréhension et l'application des règles de protection des données par les organisations, les entreprises et les autorités compétentes. En plus, cela favorise la confiance des individus dans le traitement de leurs données personnelles, en garantissant un niveau de protection uniforme et élevé quel que soit le pays où les données sont traitées. Aussi, la conformité aux normes de protection des données personnelles assure la crédibilité des organisations et des entreprises et renforce leur notoriété numérique, ce qui peut contribuer à améliorer les relations avec les individues et les partenaires, et instaurer la confiance au services numériques.

Enfin, un mécanisme de coopération internationale en matière de protection des données personnelles permet de faciliter le transfert transfrontalier de données, en réduisant les différents obstacles réglementaires et juridiques, surtout dans le domaine d'e-commerce, favorisant une concurrence équitable sur le marché mondial.

C. MÉCANISME DE COOPÉRATION ET RENFORCEMENT DE CAPACITÉS DANS LES PAYS MEMBRES DE L'ICESCO

Compte tenu des avantages d'une coopération internationale dans de protection des données personnelles, quelques soit la forme juridique, il est important de mettre en place un mécanisme et un cadre institutionnel de renforcement de la coopération entre les Etats membres de l'ICESCO. Voici quelques lignes directrices et pistes à explorer :

- Création de réseaux régionaux impliquant les Etats membres de l'ICESCO, qui interagissent avec d'autres pays à l'échelle internationale, autour de protection des données personnelles, afin de promouvoir la collaboration entre les autorités de protection des données, les gouvernements, les entreprises et les organisations de la société civile, en facilitant l'échange d'expériences, de bonnes pratiques et de ressources. De tels réseaux tiendront compte des rapprochements culturels, linguistiques et géographiques et pays membres de l'ICESCO
- Etablissement des accords de coopération bilatéraux ou multilatéraux entre les autorités de protection des données à l'échelle régionale ou interrégionale, permettant une coopération efficace pour l'échange d'informations, et également pour répondre aux notifications, aux signalements et aux enquêtes sur les incidents de sécurité des données et agir quant à la prise de de mesures appropriées. En plus, la coopération bi ou multilatérale permettra également l'adoption de normes et de bonnes pratiques communes en la matière, en favorisant la convergence des réglementations pour guider les organisations et les entreprises dans la conformité.
- Création d'un hub, forum ou conseil des réseaux régionaux, de mission globale, transverse et stratégique, afin d'harmoniser les réglementations entre les différentes régions et pays et adopter des normes communes et des bonnes pratiques de protection des données personnelles dans l'ensemble des pays membres de l'ICESCO, tout en tenant compte des différentes adhésions antérieures ou futurs des pays membres dans d'autres réseaux et groupement à l'échelle internationale ou régionale.

La mise en place d'un mécanisme institutionnel de coopération entre les Etats membres de l'ICESCO, pour le renforcement des capacités des autorités de protection des données pérsonnelles, en fournissant un cadre pour la mise en place de formation spécialisée, et un soutien aux ressources humaines pour faire face aux défis émergents en matière de protection des données, tels que la sécurité des données numériques, la protection de la vie privée et la conformité aux réglementations. En outre, promouvoir la sensibilisation et l'éducation du public sur les multiples enjeux de la protection des données personnelles et les droits des individus en matière de vie privée, afin de renforcer la confiance dans l'utilisation des technologies numériques.

6 “CONCLUSION”

A cette époque entièrement digitalisée, la protection des données personnelles est devenue une priorité essentielle. Ce guide offre une vue d'ensemble complète des principes, des bonnes pratiques et des réglementations clés en matière de protection des données personnelles, il décrit l'état de la protection des données personnelles à l'échelle internationale, et se focalise sur le cas des pays membres de l'ICESCO.

Ce guide rappelle aussi l'intérêt de l'éducation numérique dans la promotion de protection des données personnelles et la vie privée, il fournit entres autres des conseils, des bonnes pratiques et des recommandations spécifiques, il vise à aider les individus, les entreprises et les organisations à comprendre et à respecter les exigences en matière de protection des données. En sensibilisant sur les risques potentiels et en encourageant l'adoption de mesures proactives, ce guide aspire à créer un environnement numérique plus sûr et plus respectueux de la vie privée. Il souligne également l'importance de la mise en place de mécanismes de coopération internationale entres les pays membres de l'ICESCO et de la formation continue pour relever les défis relatifs de la protection des données. En fin, ce guide constitue une ressource importante pour promouvoir la culture de la confidentialité et de la sécurité des données dans la société.

7 “GLOSSAIRE TEMINOLOGIQUE”

Données personnelles : Informations qui permettent d'identifier directement ou indirectement une personne physique.

Traitement des données : Toute opération effectuée sur les données, à savoir la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation, la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion, la limitation, la destruction, etc.

Autorité de protection des données : Organisme gouvernemental indépendant chargé de surveiller le respect des lois et réglementations relatives à la protection des données personnelles.

Portabilité des données : Droit d'une personne de récupérer et de transférer ses données personnelles d'un service à un autre

Consentement : Accord explicite ou implicite d'une personne pour le traitement de ses données personnelles.

Consentement éclairé : Consentement donné par une personne après avoir reçu toutes les informations nécessaires sur le processus et les conséquences de traitement de ses données personnelles

Responsable du traitement : Personne ou entité qui détermine les finalités et les moyens du traitement des données personnelles.

Sous-traitant : Personne ou entité qui traite les données personnelles pour le compte d'un responsable du traitement de données

Droit à l'oubli : Droit d'une personne de demander la suppression de ses données personnelles, en particulier lorsque celles-ci ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées.

Droit à l'Image : Droit pour une personne de contrôler l'utilisation et la diffusion de son image.

GLOSSAIRE TEMINOLOGIQUE

Informations Profilage : Utilisation de données personnelles pour évaluer certains aspects personnels d'une personne, notamment pour analyser, ses préférences, ses intérêts, sa santé, sa situation économique, sa fiabilité ou prédire son comportement.

Transfert des données à l'étranger : Transfert de données personnelles en dehors du pays vers un pays tiers ou une organisation internationale.

Violation de données : Accès non autorisé, divulgation, altération ou destruction de données personnelles.

Anonymisation : Processus de modification des données personnelles de manière à ce qu'elles ne puissent plus être associées à une personne spécifique sans l'utilisation d'informations supplémentaires.

Chiffrement des données : Transformer les données en un format illisible, rendant ainsi leur compréhension impossible sans une clé de déchiffrement appropriée.

Cryptage de données : faire usage à un programme informatique permettant transformant les données en un format illisible pour les tiers, sauf pour ceux qui possèdent la clé de déchiffrement.

Intelligence Artificielle : Algorithmes et modèles mathématiques pour créer des systèmes capables d'apprendre et raisonner et prendre la décision à partir de données

Objet connecté à internet : dispositif physique doté de capacités de communication réseau, permettant d'interagir, transmettre et de recevoir des données via Internet

Metavers : concept de réalité virtuelle persistante et immersive où les utilisateurs interagissent entre eux et avec des environnements virtuels en temps réel.

8 LIENS UTILES

https://www.dataguidance.com/laws

https://cybersecuritymag.africa/etats-des-lieux-des-legislations-sur-protection-donnees-personnelles-afrique

https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-French.pdf

https://www.dlapiperdataprotection.com/index.html?t=law&c=SA

https://paradigmhq.org/wp- content/uploads/2023/07/Londa-2022-Gambia-Eng.pdf

https://www.dataguidance.com/opinion/brunei-darussalam-new-data-protection-regime-focus

https://help.openai.com/en/

JOIN US ! انضموا إلينا REJOIGNEZ-NOUS