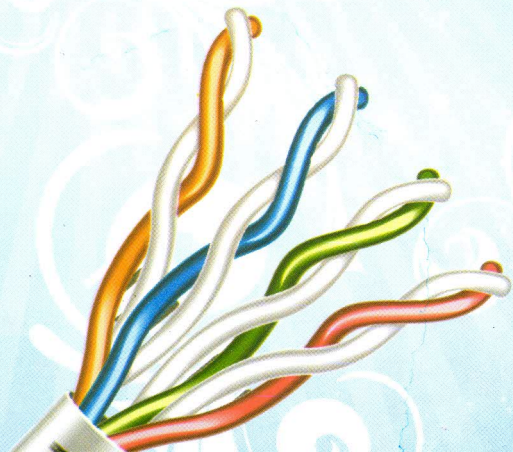
COMMISSION DE L' INFORMATIQUE ET DES LIBERTES

GUIDE

CONSEILS PRATIQUES POUR UNE MEILLEURE PROTECTION DE SES DONNEES PERSONNELLES



A LA DECOUVERTE DE LA COMMISSION DE L'INFORMATIQUE ET DES LIBERTES

1. PRESENTATION

La Commission de l'Informatique et des Libertés (CIL) est une Autorité administrative indépendante, créée par la loi n° 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel.

La Commission est composée d'un collège pluraliste de neuf (09) membres ainsi qu'il suit :

- deux magistrats représentant le pouvoir judiciaire ;
- deux députés représentant le pouvoir legislatif ;
- deux personnalités issues des associations nationales œuvrant dans le domaine des droits humains ;
- deux personnalités issues des associations nationales des professionnels de l'informatique ;
- une personnalité représentant l'éxecutif désignée par le Président du Faso.

2. QUE FAIT LA CIL ?

La CIL a pour missions essentielles de veiller à la protection des données à caractère personnel au Burkina Faso à travers la mise en œuvre de la loi sus-indiquée. Elle dispose à cet effet, d'un pourvoir réglementaire et d'un pouvoir de sanction.

A ce titre :

- la CIL est investie d'une mission générale d'information des personnes sur leurs droits et obligations en matière de traitement de données personnelles ;
- la CIL régule et récence les fichiers (à travers la déclaration et les demandes d'avis), autorise les traitements les plus sensibles avant leur mise en œuvre ;
- dans tous les secteurs d'activité (banque, assurance, éducation, commerce, santé, etc.), la CIL est appelée à aider les citoyens dans l'exercice de leurs droits, notamment le droit d'accès, de rectification et de suppression ;
- la CIL contrôle les fichiers et vérifie si les responsables de fichiers respectent la Loi portant protection des données

personnelles à travers des missions de contrôle ou de vérification ;

- la CIL peut prononcer des sanctions administratives à l'encontre des responsables de traitement qui n'ont pas respecté la Loi et faire sanctionner les infractions les plus graves par le juge (pouvoir de dénonciation) ;
- fort de son expérience, la CIL propose au Gouvernement toutes mesures législatives ou réglementaires de nature à adapter la protection des libertés à l'évolution des procédés et techniques informatiques ;
- la Commission établit et publie des normes simplifiées pour les catégories les plus courantes de traitement de données à caractère personnel qui ne comportent manifestement pas d'atteinte à la vie privée ou aux libertés individuelles ;
- les traitements de données à caractère personnel effectués par les organismes privés pour leur propre compte doivent être déclarés à la CIL avant leur mise en œuvre ;
- les traitements de données à caractère personnel opérés pour le compte de l'Etat, de ses démembrements ou pour une personne morale gérant un service public sont soumis à la CIL pour avis conforme et motivé avant l'adoption d'un décret.

3. QUELS SONT LES POUVOIRS DONT DISPOSE LA CIL ?

La Commission de l'Informatique et des Libertés dispose d'un pouvoir de contrôle et d'un pouvoir de sanction en vue d'assurer le respect effectif de la loi 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel :

- elle peut, à l'égard de tout traitement de données personnelles, procéder à des vérifications sur place au sein des organismes publics et privés et se faire communiquer tout renseignement ou document utile à sa mission ;

- elle peut prononcer des sanctions administratives (mise en demeure, interruption du traitement, verrouillage de certaines données personnelles traitées, interdiction temporaire ou définitive de la mise en œuvre d'un traitement, etc.) ;

- elle peut saisir la justice pour les infractions graves dont elle a connaissance.

4. QUE FAUT-IL SAVOIR SUR LA LOI PORTANT PROTECTION DES DONNEES A CARECTERE PERSONNEL ?

a) Notions essentielles :

- **Une donnée à caractère personnel (article 2) :** est considérée comme donnée à caractère personnel, toute information permettant d'identifier, directement ou indirectement, une personne physique, tels que son nom, son prénom, sa photo, son numéro de téléphone, son empreinte digitale...
- **Un traitement de données à caractère personnel (article 3)** : est considéré comme traitement, toute opération effectuée à l'aide de procédés informatisés ou non et appliquée à des données à caractère personnel telles que la collecte, l'enregistrement, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction.
- **Le responsable de traitement** est la personne physique ou morale qui décide de la mise en œuvre du traitement et en détermine les moyens et les finalités (article 4).
- **La personne concernée** : est toute personne dont les données font l'objet de traitement (article 4).

b) Qui fait du traitement de données à caractère personnel ?

Toute personne structure publique que privée qui, par les moyens automatisés ou manuels, collecte, traite, enregistre, extrait, consulte, utilise, transmet ou archive... des données ou des informations se rapportant aux personnes physiques, fait du traitement de données à caractère personnel.

c) Qui est concerné par le traitement de données à caractère personnel ?

Toute personne physique qui peut être amenée à communiquer ses données personnelles, soit pour bénéficier d'un service ou pour répondre à une obligation légale.

d) Les principes fondamentaux contenus dans la Loi n° 010-2004/AN du 20 avril 2004 :

- **Le principe de consentement et de légitimité (article 5) :** le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne librement son consentement.
- **Le principe de licéité et de loyauté (article 12) :** la collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse. Dans le contexte informatique et libertés, la loyauté est le fait de ne pas induire l'autre en erreur, de ne pas abuser de son consentement. La licéité c'est ce qui est permis par les textes.
- **Le principe de finalité, de pertinence, de conservation (article 14) :** les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement, de manière incompatible avec ces finalités. C'est au regard de la finalité déclarée d'un traitement que doit être appréciée la pertinence des données collectées.

- **Le principe d'exactitude (article 14) :** les données doivent être exactes, complètes et si nécessaire mises à jour. Les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées.
- **Le principe de confidentialité et de sécurité (article 15) :** le responsable du traitement doit prendre toutes les mesures pour assurer la sécurité des données. Les données ne doivent pas être divulguées ; seules les personnes autorisées peuvent y accéder.
- **Le principe de spécifiques (article 22) :** il est interdit de procéder à la collecte et à tout traitement qui révèle l'origine raciale, ethnique, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.
- **Le principe des exceptions et limitations :** les principes relatifs à la qualité des données, à l'information préalable de la personne concernée, au droit d'accès et à la publicité des traitements peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'Etat, la défense, la sécurité publique.

e) Les obligations des responsables du traitement de données :

- **Obligation de requérir l'avis de la CIL (article 18) :** les traitements de données à caractère personnel effectués pour le compte de l'Etat ou de ses démembrements doivent être soumis à la CIL pour avis motivé et conforme avant l'adoption d'un décret y afférent.
- **obligation de déclarer (article 19) :** les traitements de données à caractère personnel effectués pour le compte des organismes privés doivent être déclarés à la CIL avant leur mise en œuvre.

- **obligation de respecter, d'une manière générale tous les principes fondamentaux ci-dessus cités** dans le cadre du traitement de toute donnée à caractère personnel.

f) Les droits des personnes concernées :

- **Droit à l'information (article 13)** : le responsable du traitement doit informer toute personne qui fait l'objet du traitement dans sa structure. Concrètement, il faut informer l'individu que des données sont collectées sur lui afin qu'il y consente ou pas et donc lui fournir des réponses claires aux questions suivantes :

  1. Qui collecte mes données ?
  2. Pourquoi collecte-t-il ces données ?
  3. A qui sont destinées les données collectées ?
  4. Quels sont les renseignements obligatoires et facultatifs ?
  5. Que se passe-t-il si je ne fournis pas toutes les informations demandées ?
  6. Quelle procédure dois-je suivre à l'avenir pour rectifier ou supprimer mes données ?

- **Droit d'opposition (article 16, alinéa 2)** : la personne concernée a le droit de s'opposer, pour des raisons légitimes (manque de sécurité ou manque de confidentialité), à ce que des données la concernant fassent l'objet d'un traitement. De plus, elle peut s'opposer, sans se justifier, à ce que les données la concernant soient utilisées à des fins de prospection, en particulier commerciale.

- **Droit d'accès (article 17)** : toute personne peut demander au responsable de traitement, le droit de connaître les données conservées et traitées la concernant. Ce droit s'exerce sans délai ou frais excessifs.

- **Droit de rectification et de suppression (article 17, alinéa 3)** : toute personne peut demander à faire rectifier, compléter, actualiser, verrouiller ou effacer des données erronées la concernant.

5. QUI PEUT SAISIR LA CIL ?

Toute personne qui a intérêt, en agissant par elle-même ou par l'entremise de son avocat ou toute personne dûment mandatée peut saisir la CIL.

6. COMMENT SAISIR LA CIL ?

La CIL peut être saisie d'une plainte, d'une réclamation ou d'une pétition, par voie électronique, postale ou par le remplissage d'un formulaire prévu à cet effet et disponible à la CIL.


CONSEILS
PRATIQUES POUR
UNE MEILLEURE
PROTECTION DE
SES DONNÉES
PERSONNELLES

RISQUES, ET PRECAUTIONS LIES A LA PROTECTION DES DONNEES PERSONNELLES DANS L'UTILISATION DES TIC

La présente brochure vise à informer les citoyens sur l'existence de risques liés à l'utilisation des outils TIC. Elle propose à cet effet, des conseils à suivre afin de minimiser lesdits risques.

A. RISQUES

I. De la Téléphonie mobile

Conservation des SMS : les SMS envoyés transitent sur des serveurs SMS ; ils sont conservés pendant une période plus ou moins longue ce qui peut entrainer une insuffisance de garantie de confidentialité et d'intégrité des SMS.

Géo localisation du portable : le téléphone portable permet de localiser avec exactitude la position géographique de son propriétaire. Ce qui peut entrainer une intrusion dans sa vie privée et une perte de son intimité.

II. De la messagerie électronique (E-mail)

Insuffisance de sécurité : l'e-mail ne garantie pas toujours la sécurité et la confidentialité des messages envoyés ou reçus à partir d'un terminal non-sécurisé.

III. Des services de réseaux sociaux (Facebook, Hi5, Twitter, etc.)

L'adhésion aux différents réseaux sociaux peut entrainer :

- **une exposition de la vie privée :** toute information donnée par ce canal est souvent démultipliée ;
- **une atteinte au droit à l'image :** les photos par ce canal peuvent avoir plusieurs destinataires et être utilisées à d'autres fins à votre insu sans votre accord ;

- **une atteinte à la réputation** : toute information ou photo transmise par ce canal peut être utilisée ultérieurement en vue de salir votre réputation.

IV. Du vol de données

Vos données personnelles peuvent être usurpées lorsque vous naviguez sur internet avec des ordinateurs non sécurisés ou lorsque vous installez des logiciels gratuits (freeware), des Peer to Peer (eMule, ares, limewire, etc.) sans précaution.

V. De la perte de sécurité de son ordinateur

Le plus souvent ces risques sont causés par les virus informatiques qui peuvent corrompre ou supprimer des données de votre ordinateur.

B. CONSEILS ET PRECAUTIONS

I. Les précautions élémentaires à prendre pour une utilisation sécurisée du courrier électronique :

- avant d'ouvrir un message électronique ou une pièce jointe, assurez-vous que votre antivirus est à jour ;
- ne jamais transmettre des données confidentielles par messagerie électronique sans s'assurer de la sécurité du réseau ;
- ne jamais répondre aux spams ou courriers électroniques qui demandent des renseignements personnels (mot de passe ou information financière surtout) ;
- activer le filtre anti-spam de votre logiciel de courrier électronique.

II. Pour vos transactions en ligne notamment les opérations financières

- le faire uniquement chez des marchands dignes de confiance : pour cela, s'assurer que le site Web est légitime, que l'adresse URL est exacte, y compris le nom du domaine (com, bf, etc.) ;
- s'assurer que le marchand se sert d'un système transactionnel sécurisé. Pour savoir si un site Web est sécurisé, s'assurer que l'URL commence par https:// ou shttps:// et qu'il apparait l'icône d'un cadena verrouillé ou d'une clé intacte ;
- après avoir effectué une opération financière ou bancaire en ligne, il convient de mettre fin à la session, vider la mémoire cachée et le fichier de témoins (cookies) ;
- privilégier les sites qu'on a déjà fréquenté ou des sites recommandés.

III. Mesures et précautions à prendre lorsque vous utilisez les services de réseaux sociaux

- bien choisir quelles informations rendre visibles et avec qui les partager ;
- ne pas accepter n'importe quelle invitation d'inconnu. On peut se retrouver en relation avec d'illustres inconnus, bien intentionnés ou malintentionnés qui auront accès à nos données personnelles, e-mail, numéro de téléphone, photos de famille ou d'amis, parcours scolaire, profession, etc. (ces données personnelles peuvent être utilisées pour créer des messages d'hameçonnage, deviner votre mot de passe, usurper votre identité pour commettre éventuellement des infractions à votre insu) ;
- prendre le soin de configurer préalablement les paramètres de confidentialité ;
- s'appuyer sur la notoriété d'un éditeur avant d'intégrer un réseau social.

IV. Mesures de protection de son ordinateur

1°) Il faut installer :

- un pare-feu ;
- un logiciel anti-espion ;
- un antivirus régulièrement mis à jour.

2°) Activer l'anti hameçonnage du navigateur incorporé dans l'ordinateur.

3°) Ne pas utiliser les fonctions d'ouverture de session automatique pour sauvegarder le nom d'utilisateur et le mot de passe.

4°) S'assurer de détruire, de façon permanente, les renseignements personnels qui se trouvent sur le disque dur de son ordinateur, lorsqu'on s'en débarrasse ou le vend.

V. Les logiciels de contrôle parental

Les enfants montrent généralement une grande aisance dans l'usage de l'internet, mais il est nécessaire de les aider à avoir une utilisation raisonnée, responsable, sûre et saine, en installant sur les ordinateurs des logiciels de contrôle parental. Ces logiciels filtrent des contenus inadaptés ou inappropriés pour les adolescents.

Enfin, le meilleur moyen de protéger sa vie privée est de garder pour soi-même autant que possible ses informations personnelles confidentielles !

INTERNET N'EST PAS VOTRE CONFIDENT !

SÉCURITÉ DES TÉLÉPHONES PORTABLES ET CHIFFREMENT DES MAILS

A. SECURISER LES INFORMATIONS CONTENUES DANS SON TELEPHONE PORTABLE

Notre téléphone portable contient de plus en plus d'informations nous concernant. Pourtant, contrairement à un ordinateur, nous sécurisons peu, voire pas du tout son accès. En cas de perte ou de vol, des informations très personnelles peuvent être lues et rendues publiques.

1. Noter le numéro « IMEI » du téléphone

Le code IMEI est le numéro de série unique composé de 15 à 17 chiffres identifiant votre téléphone.

En cas de perte ou de vol, ce code sert à bloquer l'usage du téléphone sur tous les réseaux. Il est indiqué sur la boîte du téléphone quand on l'achète. Notez-le et gardez-le en lieu sûr (pas sur votre téléphone). Astuce : vous pouvez obtenir le code IMEI en tapant *#06# sur votre téléphone.

2. Toujours mettre en place un code « PIN »

Le code PIN (Personal Identification Number) est un code secret qui contrôle la carte SIM quand on allume son téléphone. Ce code verrouille le téléphone au bout de 3 codes erronés consécutifs. Il empêche l'utilisation de la carte SIM par une tierce personne, même avec un autre téléphone.

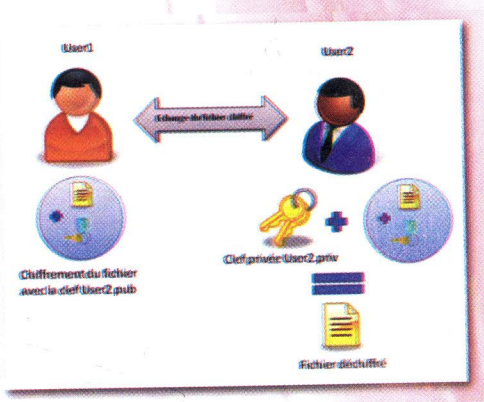
3. Mettre en place un code de verrouillage du téléphone

En plus du code PIN, ce code permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps. Cela empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol.

4. Ne pas accepter systématiquement la géolocalisation

Certains téléphones permettent de situer le lieu où nous sommes. Il est possible de contrôler quand et par qui on peut être géolocalisé. Il suffit, pour cela, de régler les paramètres de géolocalisation du téléphone ou des applications de géolocalisation (Twitter, Facebook Lieux,...). Il est également possible de désactiver ou de suspendre le service de géolocalisation à tout moment et de sélectionner les contacts qui sont autorisés à accéder aux données de localisation.

B. LE CHIFFREMENT DE SES MAILS, COMMENT ÇA MARCHE ?



Il s'agit d'un procédé utilisant un certificat électronique personnel auto signé pour chiffrer ses emails appelé chiffrement asymétrique. Cela fonctionne d'une part, avec une clé publique que vous devez communiquer à vos correspondants afin qu'ils chiffrent les mails qu'ils vous envoient. D'autre part, pour déchiffrer les mails reçus, vous avez besoin d'une clé privée qu'il vous faut garder secrète.

Mise en place du chiffrement

Des logiciels libres tels que openpgp, gpg4win, ainsi que les extensions pour firefox et Chrome (mailvelope, firepgp) permettent de créer des paires de clés et de faire le chiffrement des mails sur les webmail.


CONSEILS
PRATIQUES POUR
LA PROTECTION
DES ENFANTS
EN LIGNE

Ne laissez pas les enfants seuls face à Internet.

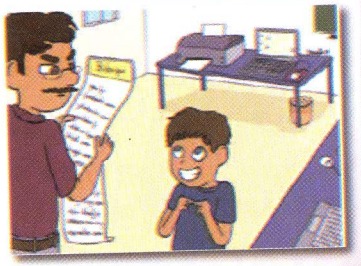
A la maison, si vous deviez ne retenir qu'une règle :

installez l'ordinateur dans la salle de séjour ou une pièce commune.

Internet doit être un outil familial et vos enfants vous sentiront présents. Si vous les laissez utiliser Internet dans leurs chambres, vous aurez plus de mal à les protéger.

Contrôlez l'accès à l'ordinateur

Lorsque vos enfants se retrouvent seuls, pensez à protéger votre ordinateur avec un mot de passe et les empêcher de se connecter à Internet en votre absence. Sachez que les adresses des sites visités sont enregistrées dans l'historique de votre logiciel « navigateur ».



Etablir un dialogue avec les enfants

Laissez vos enfants vous montrer comment ils surfent : leurs sites préférés, ceux qui pourraient vous intéresser. Invitez-les à vous montrer ce qui les gêne, discutez-en avec eux.

Eduquer les enfants à la prudence Apprenez leur des règles simples :

- ne jamais donner d'informations personnelles d'ordre privée (noms complets, adresse, téléphone);
- bien choisir un pseudonyme ;
- bien choisir les mots de passe ;
- utiliser des passephrases;
- quitter immédiatement un site qui les met mal à l'aise.

Installez un logiciel de contrôle parental

Les logiciels de contrôle parental vous permettent de filtrer l'accès à l'internet en interdisant la consultation de certaines informations sensibles ou illicites (pornographie, racisme, violence...) Des logiciels gratuits, performants et simples d'utilisation, peuvent être téléchargés (**K9 Web Protection, Windows Live Contrôle Parental**). Mais attention, ces outils ne peuvent, en aucun cas, « **REMPLACER** » la vigilance des parents ou des éducateurs.

UTILISATION DU TÉLÉPHONE MOBILE

Pour Android : un "mode enfant" pour les Smartphones ou tablettes fonctionnant sous Android, en plus des outils de sécurité standard, une application « Kid Mode » disponible sur l'Android Market permet de proposer une interface à partir de laquelle les moins de 8 ans n'auront accès qu'à des contenus adaptés.

Définissez des règles d'utilisation avec votre enfant.

Première règle : les horaires. Au même titre que l'ordinateur et la télévision, le Smartphone ne devrait pas être laissé à la disposition d'un adolescent après une certaine heure, en particulier dans sa chambre.

Deuxième règle : parlez avec l'adolescent des comportements à risques. Sexting (diffusion de photos montrant des messages inscrits sur des parties intimes du corps) et cyber-harcèlement se pratiquent le plus souvent via le mobile.

Contrôlez l'accès à Internet sur les téléphones

Sur Android, des applications comme Android Parental Control permettent de gérer les applications accessibles par l'enfant et les plannings d'utilisation.