Support de formation

✓Sécurité informatique

INSTITUT SUPERIEUR DE LA PROFESSION D'AVOCAT
Tunis

I. Sécurité Informatique

La sécurité informatique est un thème très large par rapport au contexte de ce manuel de formation.

Nous nous limiterons à l'identification des problèmes que peut affronter un utilisateur d'un ordinateur connecté à Internet et la façon de s'en prémunir.

1 Notions de sécurité et de protection de la vie privée

Travailler sur un ordinateur n'est pas une activité particulièrement dangereuse. Parler de sécurité informatique nécessite tout d'abord l'identification des objectifs, des menaces potentielles et finalement des solutions appropriées.

Les objectifs des mesures de sécurité peuvent être regroupés essentiellement sous ces 3 points :

- Préserver son ordinateur
- Préserver ses données et informations : certaines données qui se trouvent sur un ordinateur sont le fruit de long travaux (rapports d'expertise, jugements, mémoires, comptes rendus, …) les perdre est parfois très ennuyeux et représente un coût énorme.
- Préserver le caractère confidentiel de ses données et informations : certaines données stockées sont confidentielles (jugements, …) d'autres sont très personnelles (correspondance privée) et dans tous les cas il est indispensable d'éviter de les divulguer ou de se faire espionner.

Les menaces sont multiples, et elles ne sont pas nécessairement dues à de tierces parties malveillantes. Il faut les connaître pour prendre les mesures appropriées à temps. Ces menaces augmentent fortement si l'ordinateur est connecté à Internet, ce qui est généralement le cas aujourd'hui. Les principales menaces citées ici peuvent porter atteinte à un ou plusieurs des objectifs cités ci-avant.

- Les dégâts matériels accidentels ou non : coupure brusque d'électricité, surtensions sur le réseau électrique, foudre, etc.
- La suppression accidentelle de données : mauvaise manipulation, formatage accidentel du disque, pertes de données, etc.
- Les virus informatiques et dérivés : Les virus informatiques sont des logiciels dont l'objectif est de nuire à l'ordinateur et/ou aux données stockées. Ils se répondent à l'insu des utilisateurs soit à travers les CD, ou clés échangées ou les logiciels téléchargés sur internet soit à travers la messagerie électronique. Ils ont plusieurs variantes mais l'objectif est unique.
- Les logiciels espions : Ils utilisent le même mode de propagation que les virus mais leur objectif et d'envoyer à travers internet à leurs propriétaires des informations sur les logiciels installés ou sur vos habitudes sur internet (types de sites visités par exemple pour vous proposer des offres commerciales) ou encore votre carnet d'adresse ou simplement toute autre information confidentielle.

Se protéger, protéger son ordinateur et ses données et préserver leur confidentialité passe surtout par des mesures préventives à prendre et un comportement à adopter.

2 Protéger son ordinateur et ses données

2.1 Une panne peut toujours survenir

Quelque soit son origine (accident, mauvaise manipulation, virus, vol…) il faut prévoir cette éventualité et pour éviter ses conséquences sur la perte de données il faut toujours effectuer des copies de secours des données. En langage informatique on l'appelle backup. Ces backups sont primordiaux dans l'échelle des protections. Une politique de sauvegarde peut facilement être mise en place :

- D'abord identifier les dossiers à sauvegarder et ne pas éparpiller ses documents partout (le dossier mes documents et le bureau par exemple)
- Réserver une clé, un disque dur externe ou un CD réinscriptible aux backups et à rien d'autre
- Effectuer une copie des dossiers sensibles à une fréquence régulière, en fonction de la fréquence de travail sur l'ordinateur : tous les jours, toutes les semaines, mois …

Ces sauvegardes vous immunisent contre la perte des données ce qui est le plus important.

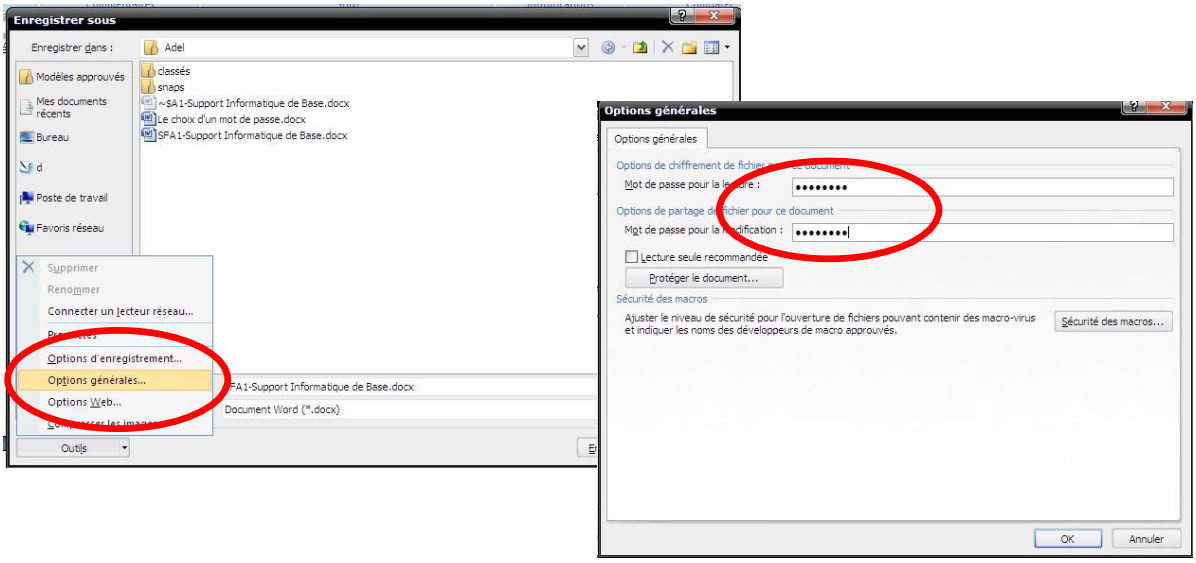
2.2 Bien gérer les utilisateurs

Si plusieurs utilisateurs travaillent sur la même machine, il faut créer des comptes différents, avec des niveaux de droit distincts et les sécuriser par des mots de passe pour garantir la confidentialité des données de chaque utilisateur. Pour cela, voir la partie gestion des utilisateurs sous Windows.

2.3 Un comportement vigilant

Si vos données sont confidentielles, il faut être vigilant :

- ne pas laisser sa machine n'importe où;
- ne pas sortir du bureau en laissant sa machine allumée (utiliser le verrouillage Ctrl +Alt+ Suppr | verrouiller l'ordinateur);
- protéger vos documents confidentiels par des mots de passe, la plupart des logiciels le permettent. Par exemple, sous MS-Word, choisir enregistrer sous puis, en bas à gauche, [outils | options générales] :



- Quand vous échangez des documents attachés à vos messages électroniques il faut être conscient que les messages peuvent être "écoutés" aussi la confidentialité des documents

échangés n'est pas assurée si vous n'utilisez pas de moyens supplémentaires.

2.4 Choix et mémorisation des mots de passe

Beaucoup de mesures de sécurité utilisent les mots de passe. Le mot de passe est la clé de voute de tout système de sécurité, il doit être bien choisi pour ne pas être "craqué" facilement, on l'appellera alors un mot de passe fort. Voici quelques conseils utiles pour le choix et la manipulation des mots de passe :

- Privilégier un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres. Il est plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.
- Eviter les mots triviaux, les prénoms, les nombres et les mots du dictionnaire.
- Utiliser un mot de passe d'au moins 8 caractères, 10 c'est encore mieux.
- Choisir un mot de passe facile à retenir. En effet, si le mot de passe est trop compliqué à retenir, vous serez tenté par exemple de l'inscrire sur un papier collé sur l'écran ou sous le clavier ou sur votre portefeuille. Pour trouver un mot de passe facile,
    - on peut utiliser la mémorisation phonétique, c.-à-d. utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « J'ai acheté neuf cd neufs pour cent Dinars cet après midi » deviendra ght9CD9%d7am;
    - on peut également utiliser la méthode des premières lettres d'une phrase simple (citation, parole de chanson...) en mélangeant minuscules et majuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.
- Ne pas divulguer son mot de passe. Un mot de passe ne doit jamais être partagé ni stocké dans un fichier ni sur papier ni envoyé par mail, il faut le retenir par cœur.
- Ne jamais utiliser l'option "retenir le mot de passe" que vous proposent certains logiciels comme les navigateurs internet. D'abord on n'est jamais sûr où est ce que ce sera stocké et puis on les oublie si on ne les utilise pas.
- Ne pas utiliser le même mot de passe pour toutes vos protections, "on ne met pas tous ses œufs dans le même panier".

3 Se protéger contre les menaces du monde numérique

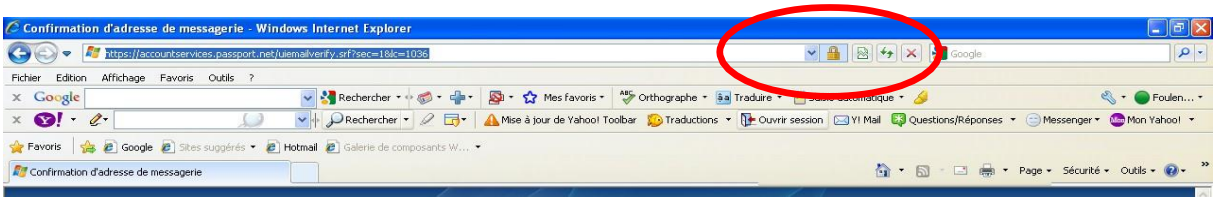
Naviguer sur internet, utiliser sa messagerie électronique ou instantanée, télécharger des logiciels sont autant d'activités classiques sur internet mais qui comprennent certains risques qu'il faut connaître et éviter.

3.1 Transactions sécurisées

Lorsque des informations confidentielles (mots de passe, numéros de comptes, de cartes bancaires, etc.) sont saisies sur des pages Web, il faut d'abord éviter de le faire sur des sites douteux et il faut s'assurer que la transaction est sécurisée pour éviter les écoutes sur le réseau. Le cadenas vert à droite de la barre d'adresse de votre navigateur vous indique que la transaction est sécurisée. Si ce cadenas n'apparaît pas lors de la visite d'un site, il faut éviter de saisir des informations confidentielles.

3.2 Attention aux pièces jointes

La messagerie électronique ou instantanée permet d'échanger des documents attachés aux messages. C'est la faille qu'utilisent plusieurs virus pour se répandre. Lorsqu'on reçoit un message non sollicité comprenant une pièce jointe il faut être très vigilant :



- Il ne faut jamais exécuter un logiciel arrivant en pièce jointe.

- Ne jamais ouvrir une pièce jointe non sollicitée avant de s'assurer que son expéditeur l'ait envoyé intentionnellement. Beaucoup de virus, une fois installés sur une machine, utilisent la messagerie pour s'auto-envoyer en pièce jointe avec un message amical banal à tous les contacts se trouvant cette machine.

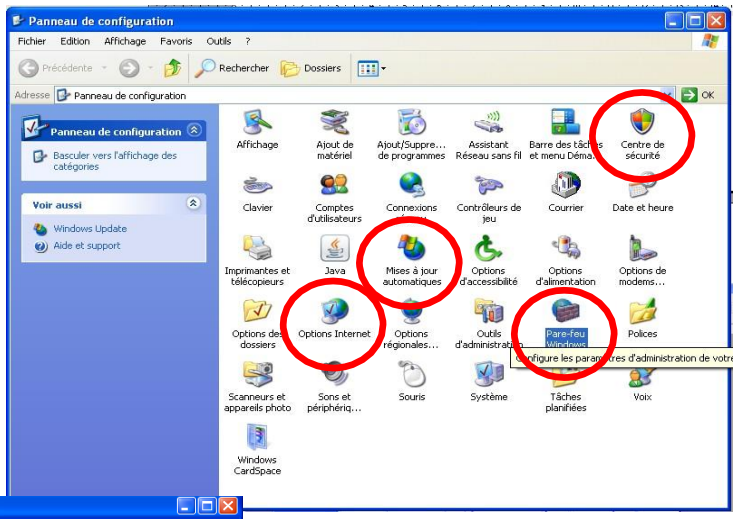
3.3 Attention à l'hameçonnage

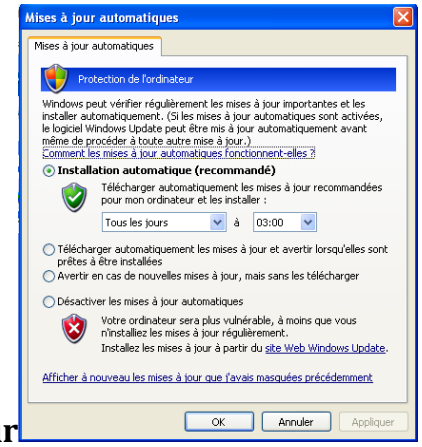
Les messages d'hameçonnage sont des messages électroniques ayant une apparence très sérieuse et dont l'objectif final, d'une façon ou d'une autre, est de vous amener à saisir ou envoyer des informations confidentielles comme des mots de passe, numéros de cartes bancaires, etc. Cela peut prendre la forme d'un appel au secours, d'un message d'un riche fils d'un banquier persécuté dans son pays qui vous demande de l'aider à transférer sa fortune moyennant une large récompense, ou d'un message du directeur informatique de votre banque qui vous demande de saisir votre mot de passe et de le modifier pour des raisons de sécurité, etc, les exemples sont nombreux. Comme partout, sur Internet également il ne faut pas être crédule. La règle est simple : ne jamais répondre aux messages vous invitant à remplir des formulaires ou d'envoyer des informations confidentielles avant de s'assurer de l'expéditeur.

4 Garder son ordinateur protégé et à-jour

Le bon paramétrage du système d'exploitation de votre machine et quelques logiciels supplémentaires comme un antivirus, un antispyware et un firewall et enfin un bon comportement peuvent être un très bon moyen de lutte contre tous les risques qui menacent votre machine, vos données, et leur confidentialité.

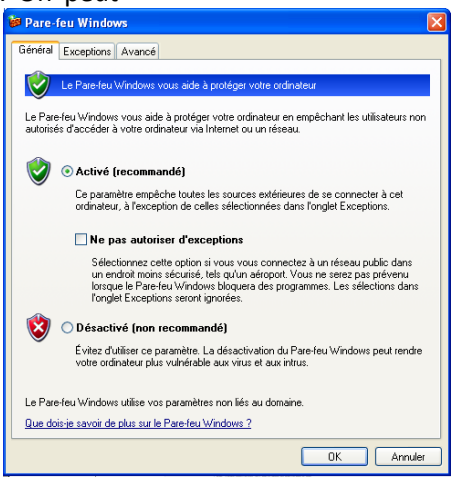
Le paramétrage du système d'exploitation commence toujours par le panneau de configuration qui comprend les éléments à paramétrer. Le centre de sécurité vous donne accès à ces éléments en vous fournissant également des conseils sur la sécurité de votre machine.





4.1 Les mises à jour

L'outil de mises à jour automatiques vous permet de configurer votre ordinateur pour se connecter aux serveurs de Microsoft et télécharger les mises à jour. Ces mises à jour sont gratuites et très utiles. En effet les virus et les techniques d'intrusion évoluent et chaque fois qu'on détecte de nouvelles failles exploitables pour nuire à la sécurité des machines des correctifs sont mis au point. Il est préférable d'être à jour de ce point de vue. On peut Choisir un niveau moyen en demandant d'être prévenu chaque fois qu'une mise à jour est prête et de décider soi-même de l'installer ou non.

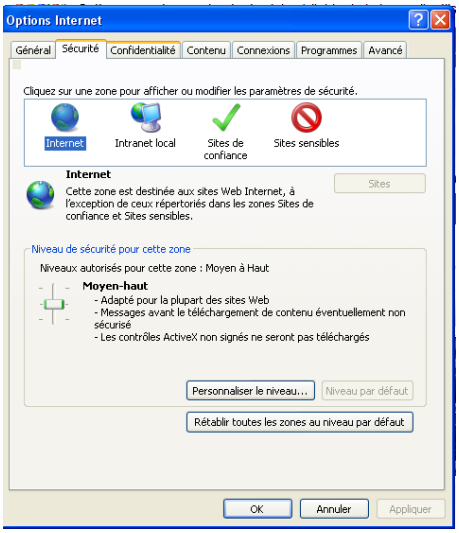


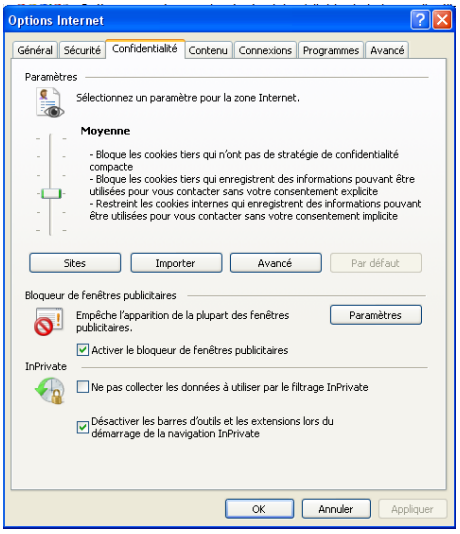
4.2 Le Pare-feu (Firewall)

Une machine connectée à Internet est une cible potentielle. Le firewall est un logiciel qui filtre toutes les données entrantes et sortantes de votre machine et vous prévient en cas d'information entrante ou sortante non attendue. Par exemple, il est possible d'avoir un cheval de Troie sur sa machine : un logiciel qu'on a installé qui est supposé faire un travail donné et qui à l'insu des utilisateurs renvoient des informations (confidentielles ou non) vers un serveur. Le Firewall permet de détecter ce genre d'activité et vous prévient. Vous pouvez alors bloquer les messages. Le paramétrage d'un firewall nécessite certaines connaissances en informatique mais il est quand même très utile de l'activer et de choisir le paramétrage par défaut.

4.3 Les options internet

Le module "options internet" du "centre de sécurité" comprend également 3 volets paramétrables qui nous intéressent : le volet "sécurité", le volet "confidentialité" et le volet "contenu".

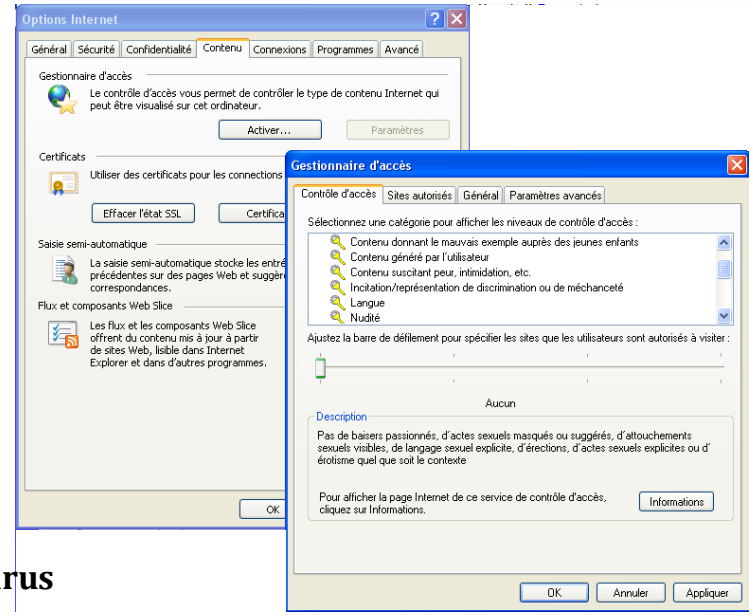




Dans le volet "Sécurité" 3 niveaux de sécurité sont définis. En choisissant le niveau le plus haut chaque activité à risque est signalée. L'utilisation du navigateur en devient parfois ennuyeuse.

Dans le volet "Confidentialité" on peut régler la sensibilité de la machine aux cookies. Ce sont des fichiers laissés sur votre machine par les sites visités et dont l'objectif premier est de "connaître votre profil pour mieux vous servir". Ceci constitue déjà une atteinte à la vie privée des internautes. On peut choisir d'autoriser ou non ces cookies en manipulant le niveau de confidentialité de ce volet.

Dans le volet "Contenu" il est possible d'interdire l'accès à un type de site ou à un type de contenu ou à des sites spécifiques en donnant leurs adresses. Ceci peut être utile dans le cadre d'un contrôle parental, par exemple, sur les sites vus par les enfants.



4.4 Installer un antivirus

Un antivirus est un élément fondamental dans la sécurisation d'un ordinateur. Il permet de lutter contre les virus (et toutes leurs variantes) en particulier et d'améliorer le niveau de sécurité et de confidentialité de la machine. Les antivirus sont nombreux, il est primordial d'en choisir un qui est mis à jour régulièrement à travers la connexion internet : de nouveaux virus sont découverts tous les jours. Certains antivirus offrent plusieurs services supplémentaires comme les antispyware, firewall, anti-fenêtres publicitaires (pop up), etc.

Le site web de l'agence nationale de la sécurité informatique est une très bonne adresse. A part les informations générales, on y trouve une sélection d'outils logiciels gratuits (antivirus et autres) on y trouve également des informations à jour concernant les précautions particulières à prendre.

II. Ethique informatique

"La règle de conduite dans la vie réelle doit être la même quand on est face à sa machine". "Internet n'est pas un bouclier derrière lequel on peut tout se permettre". Ces deux phrases résument ce qu'on appelle éthique informatique, il n'y a pas une éthique spécifique à l'informatique mais simplement un rappel des règles qui sont de rigueur ailleurs. Il est parfois utile de rappeler certains points :

- Respect de la confidentialité et des espaces personnels
- Respect de la propriété intellectuelle
- Ne pas mettre en danger la sécurité personnelle ou du groupe
- Ne pas falsifier les données ou logiciels
- Ne pas nuire ou menacer
- Pour tout ce qui concerne la publication d'information : même éthique que la presse : respect de la dignité des personnes, respect des libertés, pas de diffamation...

A propos de la propriété intellectuelle, il est peut être utile de rappeler que le logiciel est le résultat d'un travail et qu'il est protégé par le droit d'auteur. Aussi, faut-il garder à l'esprit que, même si l'opération est très facile à faire, copier un logiciel ou le distribuer a des fin commerciales ou non est interdit par la loi!

De même, un document publié sur internet (articles, livres, musique, films, etc.) est la propriété de son auteur. L'utiliser nécessite au moins la citation de son origine sinon l'autorisation de l'auteur.

1 Comment lutter contre la cybercriminalité ?

La cybercriminalité est l'ensemble des infractions pénales réalisées via les réseaux informatiques, en particulier sur le réseau internet. Elle est constituée à la fois par des atteintes aux biens tels que la fraude sur les cartes bancaires, le piratage d'ordinateurs, etc…Face à de tels dangers, les actions de lutte contre cette tendance se multiplient, mais les spécialistes sont encore loin de pouvoir l'éradiquer ou de réduire le taux d'infractions criminelles perpétrées !

Partant par cette optique, le ministère des Technologies de l'Information et de la communication, a annoncé la création officielle de l'Agence technique des télécommunications (ATT) en vertu du décret 4506 en date du 6 novembre 2013. Il s'agit d'une institution publique à caractère administratif et indépendante financièrement mais placée sous la tutelle du ministère des TIC, ayant vocation à fournir l'assistance technique aux enquêtes judiciaires concernant la lutte contre la cybercriminalité. Ainsi elle veille sur la protection des citoyens et des intérêts supérieurs du pays 24h/24 et 7jours/7, conformément à la loi et sous contrôle judiciaire.

L'agence veille, également, à renforcer les principes de respect des droits de l'homme et contribuera à l'établissement des garanties nécessaires pour protéger les données personnelles et mettre en place des règles de transparence dans les enquêtes sur les crimes du cyberspace.

Le département des TIC a mis en place un ensemble de garanties juridiques, procédurales,

structurelles, réglementaires et de contrôle dans l'objectif de consacrer, dans le cadre des activités de l'agence, le principe du respect des droits de l'homme, la protection des données personnelles, la liberté d'expression sur Internet et le droit d'accès libre à l'information.

III. Projet de loi cybercrime

مشروع قانون
يتعلق بمكافحة جرائم أنظمة المعلومات والاتصال

الباب الأول
أحكام عامّة

الفصل الأول:

يهدف هذا القانون إلى التوقي من **جرائم أنظمة المعلومات والاتصال** وزجرها وضبط الأحكام الخاصة بجمع الادلة الكترونية.

وتنطبق على الجرائم المنصوص عليها بهذا القانون أحكام المجلة الجزائية ومجلة الإجراءات الجزائية ومجلة المرافعات والعقوبات العسكرية والنصوص الجزائية الخاصة بقدر ما لا تتعارض مع أحكامه.

ويخضع الأطفال إلى مجلة حماية الطفل.

الفصل 2:

يُقصد بالمصطلحات التالية على معنى هذا القانون:

- نظام معلومات: مجموعة برمجيات وأدوات وأجهزة منعزلة أو مرتبطة فيما بينها أو متصلة ببعضها البعض تقوم بعمليات المعالجة الآلية للبيانات.
- بيانات معلوماتية: كل عرض للوقائع أو للمعلومات أو للمفاهيم في شكل قابل للمعالجة الآلية بما في ذلك البرمجيات التي تُمكّن نظام معلومات من وظيفة معينة.
- مزوّد خدمات اتصال: كل شخص طبيعي أو معنوي يقوم بإسداء خدمة اتصالات بما في ذلك خدمات الانترنات على معنى مجلة الاتصالات.
- حركة الاتصال أو بيانات المرور: بيانات ينتجها نظام معلومات تُبيّن مصدر اتصال والوجهة المرسل إليها والطريق الذي سلكه وساعته وتاريخه وحجمه ومدته ونوع خدمة الاتّصال

- حامل معلوماتي: هو وعاء أو جهاز لتخزين المعلومات يمكن تنصيبه وازالته من الحاسوب ويستعمل غالبا لنقل البيانات كالذواكر الوميضية والاقراص المرنة أو الليزرية وغيرها
- البرمجية : صياغة البيانات والإجراءات وأدلة التعليمات الفنية التي تؤدي مهمة ما في نظام تشغيل الحاسب.

الباب الثاني
في بعض الواجبات والإجراءات الخاصّة

القسم الأول
في واجب حفظ البيانات

الفصل 3:

يتعيّن على مزوّدي خدمات الاتصال كل في حدود الالتزامات المحمولة عليه بمقتضى الأحكام التشريعية والترتيبية الجاري بها العمل أن يحفظوا البيانات المخزّنة في نظام معلومات لمدّة سنة واحدة ابتداء من تاريخ التسجيل.

تتمثل البيانات الواجب حفظها في ما يلي :

- البيانات التي تمكّن من التعرّف على مستعملي الخدمة،
- البيانات المتعلقة بحركة الاتصال،
- البيانات المتعلقة بالأجهزة الطرفية للاتصال.

القسم الثاني
في معاينة الجرائم وتنفيذ أذون الاعتراض والنفاذ

الفصل 4:

يتولى معاينة الجرائم المنصوص عليها بهذا القانون كل في حدود اختصاصه:

- مأمورو الضابطة العدلية المشار إليهم بالعددين 3 و4 من الفصل 10 من مجلة الإجراءات الجزائية و مأمورو الضابطة العدلية العسكرية المنصوص عليهم بالعدد 3 من الفصل 16 من مجلة المرافعات والعقوبات العسكرية.

- الأعوان المحلّفون للوزارة المكلّفة بتكنولوجيا المعلومات والاتصال المؤهّلين للغرض المنصوص عليهم بمجلة الاتصالات.

الفصل 5:

تتولى الوكالة الفنية للاتصالات تأمين الدعم الفني لتنفيذ الأذون المتعلقة بالنفاذ إلى المعطيات المخزنة بقواعد البيانات أو جمع بيانات حركة اتصالات أو اعتراض محتوى الاتصالات ونسخها أو تسجيلها.

وعلى مزودي خدمات الاتصال التعاون مع الوكالة الفنية ومساعدتها على تنفيذ مهامها كل حسب نوع الخدمة التي يسديها.

وتتولى الوكالة تحرير محضر إداري في عمليات النفاذ أو الجمع التي أنجزتها يتضمن وجوبا البيانات التالية:

- نص الإذن الذي كلفت بتنفيذه،
- الترتيبات الفنية التي قامت بها لتنفيذ الإذن و نوع المساعدة التي تلقتها من مزودي الخدمات،
- التدابير الفنية التي اتخذتها الوكالة لحفظ البيانات التي تم جمعها و تأمين صحتها وسلامتها في كافة المراحل،
- تاريخ بداية العمليات ونهايتها يوما وساعة.

ويرفق المحضر بنتائج عمليات النفاذ أو الاعتراض وكذلك البرامج والبيانات الفنية الضرورية التي تؤمن حفظها واستغلالها دون التأثير على صحتها وسلامتها.

الفصل 6 :

تحال نتائج عمليات النفاذ أو الاعتراض والمعطيات الفنية الملحقة بها على الجهات المعنية التي وقع تحديدها بإذن النفاذ أو الاعتراض للاستغلال.

و إذا كان الغرض من النفاذ أو الاعتراض وقائيا يحرر الهيكل المكلف بتلقي نتائج عمليات النفاذ والاعتراض و تحليلها محضرا إداريا يتضمن وجوبا البيانات التالية:

- نص الاذن الذي كلفه بمعالجة نتائج عمليات النفاذ والاعتراض،
- تاريخ تلقيه للنتائج،
- وصفا إجماليا لتلك النتائج من حيث النوع والحجم أو السعة و الشكل ومرفقاتها،

- التدابير الادارية والفنية التي اتخذت للحفاظ على صحة وسلامة المعطيات المتحصل عليها،
- هويات الاشخاص المتدخلين في استغلال تلك النتائج وصفاتهم وإمضاءاتهم بكل صفحة من المحضر.

يجب على الهياكل المعنية الاحتفاظ بالمحاضر الادارية لمدة لا تقل عن العشرة أعوام ولو في صورة تدمير النتائج بعد الاستيفاء الحاجة منها أو إحالتها على العدالة.

القسم الثالث
في جمع الأدلّة

الفصل 7:

لوكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك، حسب الحالات، أن يأمروا بتمكينهم من البيانات المعلوماتية المخزّنة بنظام أو حامل معلوماتي أو المتعلّقة بحركة اتصالات أو بمستعمليها أو غيرها من البيانات التي من شأنها أن تساعد على كشف الحقيقة.

الفصل 8:

لوكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك، حسب الحالات، أن يأذنوا بالنفاذ مباشرة أو بالاستعانة بمن يرونه من أهل الخبرة إلى أي نظام أو حامل معلوماتي وإجراء تفتيش فيه قصد الحصول على البيانات المخزّنة التي من شأنها أن تساعد على كشف الحقيقة.

الفصل 9 :

لوكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك، حسب الحالات، الإذن بحجز كامل نظام معلومات أو جزء منه أو حامل معلوماتي من شأنها أن تساعد على كشف الحقيقة.

وإذا لم يكن حجز نظام المعلومات ضروريا أو تعذّر إجراءه، تنسخ البيانات التي لها علاقة بالجريمة والبيانات التي تؤمّن قراءتها وفهمها على حامل معلوماتي.

تتّخذ الاحتياطات الضرورية للحفاظ على سلامة البيانات المحجوزة بما في ذلك الوسائل الفنية لحماية محتواها.

الفصل 10:

تحرّر قدر الإمكان قائمة في المحجوز بحضور ذي الشبهة أو من وجد لديه المحجوز ويحرّر تقرير في الحجز.

تحفظ الأشياء المحجوزة، حسب الحالة، في ظرف أو ملف مختوم و تكتب عليه ورقة مع بيان تاريخ الحجز وساعته وعدد المحضر أو القضية.

الفصل 11:

إذا استحال إجراء الحجز بصفة فعلية يتعيّن، حفاظا على أدلّة الجريمة، استعمال كافّة الوسائل المناسبة لمنع الوصول والنفاذ إلى البيانات المخزّنة بنظام معلومات.

الفصل 12:

لوكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك، حسب الحالات، الإذن بالجمع أو التسجيل الفوري لبيانات حركة اتصالات باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك، عند الاقتضاء، بمزودي الخدمات كلّ حسب نوع الخدمة التي يسديها.

الفصل 13:

لقاضي التحقيق أن يأذن **بالاعتراض الفوري** لمحتوى اتصالات وتسجيلها أو نسخها .

ويتضمّن قرار قاضي التحقيق جميع العناصر التي من شأنها التعريف بالاتصالات موضوع طلب الاعتراض والأفعال الموجبة له ومدّته.

الفصل14:

لا يمكن أن تتجاوز مدّة الاعتراض ثلاثة أشهر بداية من تاريخ الشروع الفعلي في إنجازه قابلة للتمديد مرة واحدة بمقتضي قرار معلل من قاضي التحقيق المتعهد بالقضية

ويتعين على الجهة المكلفة بتنفيد إذن الإعتراض إعلام قاضي التحقيق بالتاريخ الفعلي لانطلاق عملية الاعتراض والتنسيق معه بخصوص إتخاذ التدابير اللازمة لحسن سيرها.

الباب الثالث

في الجرائم المتّصلة بأنظمة المعلومات والاتصال

القسم الأول

في الاعتداء على سلامة أنظمة المعلومات والبيانات وسرّيتها

الفصل 15:

يعاقب بالسجن مدّة عام وبخطية قدرها عشرة آلاف دينار كل من يتعمّد النّفاذ أو البقاء عن غير وجه حق بكامل نظام معلومات أو بجزء منه.

ويستوجب نفس العقاب كل من يتعمّد تجاوز حدود حق النّفاذ الممنوح له.

والمحاولة موجبة للعقاب.

الفصل 16:

يعاقب بالسجن مدّة عامين وبخطية قدرها عشرون ألف دينار كل من يتعمّد، عن غير وجه حق، استخدام وسائل فنّية لاعتراض بيانات اتّصال بمناسبة إرسال غير موجه للعموم داخل نظام معلومات أو انطلاقا منه أو في اتجاهه بما في ذلك ما ينبعث من نظام المعلومات من إشعاعات كهرومغناطسية ناقلة لبيانات الاتصال.

ويشمل الاعتراض الحصول على بيانات حركة الاتصالات محتواها وكذلك نسخها أو تسجيلها.

والمحاولة موجبة للعقاب.

الفصل 17:

يعاقب بالسجن مدّة عامين وبخطية قدرها عشرون ألف دينار كل من يتعمّد إنتاج أو بيع أو توريد أو توزيع أو توفير أو عرض أو الحصول بغرض الاستعمال أو حيازة ما يلي:

– جهاز أو برنامج معلوماتي صُمّم أو طُوّع لارتكاب الجرائم المنصوص عليها بهذا القانون،

– كلمة عبور أو رمز نفاذ أو أي بيانات معلوماتية مماثلة تُمكّن من النفاذ إلى كامل نظام معلومات أو جزء منه بغرض ارتكاب الجرائم المنصوص عليها بهذا القانون.

والمحاولة موجبة للعقاب

الفصل 18:

يعاقب بالسجن مدة ثلاثة أعوام وبخطية قدرها ثلاثون ألف دينار كل من يتعمّد إلحاق ضرر ببيانات معلوماتية أو تغييرها أو فسخها أو إلغائها أو تدميرها.

والمحاولة موجبة للعقاب.

الفصل 19:

يعاقب بالسجن مدة خمسة أعوام وبخطية قدرها ثلاثون ألف دينار كل من يتعمّد إختلاس بيانات معلوماتية.

والمحاولة موجبة للعقاب.

وتطبق على الأفعال المنصوص عليها بالفقرة الأولى ظروف تشديد جريمة السرقة المقررة بالمجلة الجزائية.

الفصل 20:

يعاقب بالسجن مدّة ستّة أعوام وبخطية قدرها خمسون ألف دينار كل من يتعمد عن غير وجه حق إعاقة عمل نظام معلومات بإدخال بيانات معلوماتية أو إرسالها أو إلحاق ضرر بها أو تغييرها أو فسخها أو إلغائها أو تدميرها.

ويمكن للمحكمة أن ترفع الخطية إلى ما يعادل قيمة الضرر.

ويضاعف العقاب إذا ارتكبت الأفعال المذكورة بمناسبة مباشرة نشاط مهني أو ألحقت أضرارا بمصالح حيوية للدولة.

القسم الثاني

في الجرائم المرتكبة بواسطة أنظمة أو بيانات معلوماتية

الفرع الأول

الاحتيال المعلوماتي

الفصل 21:

يعاقب بالسجن مدّة ستّة أعوام وبخطية قدرها خمسون ألف دينار كل من يتعمّد إلحاق ضرر بالذمة المالية للغير بإدخال بيانات معلوماتية أو تغييرها أو فسخها أو إلغائها أو

بالاعتداء بأي وجه من الأوجه، على عمل نظام معلومات قاصدا بذلك الحصول على منافع مادية أو اقتصادية لنفسه أو لغيره.
ويضاعف العقاب إذا ارتكبت الأفعال المبيّنة بالفقرة المتقدّمة بمناسبة مباشرة نشاط مهني.

الفرع الثاني
التدليس المعلوماتي

الفصل 22:

يعاقب بالسجن مدّة عشرة أعوام وبخطية قدرها مائة ألف دينار كل من يتعمد ارتكاب تدليس من شأنه إلحاق ضرر بإدخال بيانات معلوماتية أو تغييرها أو فسخها أو إلغائها ترتّب عنه بيانات غير صحيحة قصد اعتمادها كما لو كانت صحيحة.
ويضاعف العقاب إذا ارتكبت الأفعال المبيّنة بالفقرتين المتقدمتين بمناسبة مباشرة نشاط مهني.

القسم الثالث
في جرائم المحتوى المعلوماتي غير المشروع

الفصل 23 :

يعاقب بالسجن مدّة ستة أعوام وبخطية قدرها خمسون ألف دينار كل من يتعمّد إنتاج أو عرض أو توفير أو نشر أو إرسال أو الحصول أو حيازة بيانات معلوماتية ذات محتوى إباحي يتعلق بطفل سنه أقل من 18 سنة كاملة.
ويعدّ محتوى إباحيا على معنى الفقرة المتقدّمة كلّ البيانات التي تظهر طفلا أو شخصا يبدو في مظهر طفل بصدد القيام بإيحاءات أو ممارسات جنسية أو يتعرض لها.

الفصل 24:

يعاقب بالسجن مدّة ستة أشهر وبخطية قدرها خمسة آلاف دينار كلّ من يتعمد استعمال نظام معلومات أو اتصال لترويج بيانات ذات محتوى يشكل تجاهرا بفحش أو اعتداء على الأخلاق الحميدة.

ويكون العقاب بالسجن لمدة ثلاثة أعوام وبخطية قدرها عشرة ألاف دينار إدا كان محتوى البيانات يرمي إلى التحريض على الخناء أو الفجور.

الفصل 25:

يعاقب بالسجن مدّة خمسة أعوام وبخطية قدرها خمسون ألف دينار كل من يتعّمد استعمال نظام معلومات في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للأخلاق الحميدة أو لإظهارها بطريقة من شأنها هتك شرفه أو المساس من اعتباره.

والمحاولة موجبة للعقاب.

القسم الرابع

في زجر الإخلال بموجبات جمع الأدلة الإلكترونية

الفصل 26:

يعاقب بالسجن مدّة عام وبخطية قدرها عشرة آلاف دينار أو بإحدى هاتين العقوبتين مزوّد الخدمات الذي لا يلتزم بواجب الحفظ المحمول عليه بموجب أحكام الفصل 3 من هذا القانون.

الفصل 27:

يعاقب بالسجن مدّة عام وبخطية قدرها عشرة آلاف دينار كل من يعيق سير البحث برفض تسليم بيانات معلوماتية أو وسائل النفاذ إليها لقراءة البيانات المحجوزة وفهمها أو يتعمّد إعدامها أو إخفاءها قبل حجزها.

الفصل 28:

يعاقب بالسجن مدّة عامين وبخطية قدرها عشرون ألف دينار كلّ من يتعمّد بأي وجه انتهاك سرّية الإجراءات المتعلقة بجمع أو اعتراض أو تسجيل بيانات حركة اتصالات أو محتواها أو إفشاء البيانات المتحصل عليها أو استعمالها عن غير وجه حق.

القسم الخامس

في المسؤولية الجزائية للذوات المعنوية

الفصل 29:

تنسحب العقوبات المنصوص عليها بهذا القانون على مسيّري الذوات المعنوية وعلى ممثليها إذا ثبتت مسؤوليتهم الشخصية عن الأفعال المستوجبة لهذه العقوبات.

ولا يمنع ذلك من تتبع هذه الذوات إذا تبيّن أن الجرائم المرتكبة تمّت لفائدتها أو حصلت لها منها مداخيل أو كانت تمثّل الغرض منها.

ويكون العقاب بخطية تساوي خمس مرّات قيمة الخطية المستوجبة للذوات الطبيعية.

كما يمكن للمحكمة أن تقضي بحرمان الذات المعنوية من مباشرة النشاط لمدّة أقصاها خمسة أعوام أو أن تقضي بحلّها.

الباب الرابع

في تدابير الأمن العام والدفاع الوطني

القسم الأول

في بعض الإجراءات الوقائية

الفصل 30:

يمكن للسلطات العمومية المكلفة بحماية الأمن العام والدفاع الوطني أن تتولى استثنائيا وفقا لأحكام الباب الرابع من هذا القانون النفاذ إلى البيانات المخزنة بقواعد البيانات العامة والخاصة أو جمع بيانات حركة اتصالات أو اعتراض محتوى اتصالات ونسخها أو تسجيلها وذلك بغرض التوقي من الجرائم المنظمة أو الإرهابية أو الاعتداء على أمن الدولة وفي الحالات التي تتوفر فيها معطيات عن وجود مخاطر محتملة من شأنها أن تهدد المصالح الحيوية للدولة.

الفصل 31:

يَجوز لوزير الداخلية أو الدفاع الوطني أن يأذن كتابيا بالنفاذ إلى المعطيات المتعلقة بالتعريف بمستعملي خدمات الاتصال أو بجمع بيانات حركة اتصالات.

ويحجر استعمال المعطيات التي وقع جمعها في غير الأغراض المحددة بالإذن كما يمنع إحالتها لغير السلطات العمومية المكلفة بإنفاذ القانون.

الفصل 32:

يجوز لوزير الداخلية أو لوزير الدفاع الوطني أن يأذن كتابيا بالنفاذ إلى محتوى البيانات المخزنة بقواعد البيانات العامة والخاصة أو الاعتراض الحيني لمحتوى اتصالات ونسخها أو تسجيلها.

يتضمن الإذن وجوبا أسبابه وأهدافه ومدته والجهة المكلفة باستغلال النتائج.

ويمنح الإذن لمدة أقصاها ستة أشهر قابلة للتمديد مرة واحدة لنفس المدة وفقا لنفس الإجراءات.

ويحال الإذن وجوبا على رئيس الحكومة في أجل أقصاه يومان من تاريخه.

يتخذ رئيس الحكومة في أجل اقصاه 4 أيام من تاريخ توصله بالإذن قرارا في المصادقة عليه أو رفضه يتم تبليغه فورا بأي وسيلة تترك أثرا كتابيا.

وفي صورة الرفض تتوقف فورا كل عمليات النفاذ أو الاعتراض التي شرع في تنفيذها وتدمر كل البيانات المتحصل عليها منذ انطلاقها.

يحجر استعمال المعطيات التي وقع جمعها في غير الأغراض المحددة بالإذن ويمنع إحالتها لغير السلطات العمومية المكلفة بإنفاذ القانون.

الفصل 33:

اذا لم يترتب عن المعطيات أو البيانات المتأتية من عمليات النفاذ أو الجمع أو الاعتراض تتبعات جزائية أو وقع رفض المصادقة على إذن الاعتراض يأمر الوزير الذي أصدر الإذن الجهات التي كلفها باستغلال البيانات والمعطيات المجمعة بتدميرها كليا أيا كان حاملها المادي .

ويحرر في تلك العملية محضرا إداريا يتضمن وجوبا البيانات التالية:

- نص الاذن وعند الاقتضاء قرار المصادقة أو الرفض المتعلق به
- بيانات المحضر الاداري الذي حررته الوكالة الفنية والمحضر الاداري الذي حرره الهيكل المعني باستغلال النتائج
- وصفا إجماليا لحالة النتائج من حيث النوع والحجم أو السعة و الشكل ومرفقاتها
- البيانات المتعلقة بأمر التدمير
- هويات الأشخاص المكلفين بالتدمير وصفاتهم وإمضاءاتهم بكل صفحة من المحضر.

- وصفا دقيقا لمراحل عملية التدمير
- تاريخ العملية يوما وساعة.

القسم الثاني
في الهيئة التونسية لمراقبة الاعتراض على أنظمة الاتصال والمعلومات

الفصل 34:

تحدث هيئة عمومية مستقلة تتمتع بالشخصية المعنوية والاستقلال الإداري والمالي مقرها تونس العاصمة تسمى " الهيئة التونسية لمراقبة الاعتراض " ويشار إليها في هذا القانون بعبارة "الهيئة".

تكلف الهيئة بمراقبة احترام إجراءات تنفيذ عمليات النفاذ إلى قواعد البيانات والاعتراض على حركة الاتصالات ومحتواها.

يضبط بأمر التنظيم الإداري والمالي للهيئة.

الفصل 35:

تحال الأذون المتعلقة بالنفاذ الى قواعد البيانات الخاصة والعامة أو جمع بيانات حركة اتصالات أو اعتراض محتوى اتصالات ونسخها وتسجيلها على الهيئة في أجل أقصاه سبعة أيام من تاريخ صدورها.

وتتولى الهيئة مراقبة احترام الاذون للإجراءات المقررة أعلاه

كما تحال جميع المحاضر الادارية المحررة عند تنفيذ عمليات النفاذ او الاعتراض من الوكالة الفنية أو من الهيكل المعني باستغلال نتائج تلك العمليات على الهيئة في أجل أقصاه خمسة عشر (15) يوما من تاريخ ختمها.

وتتولى الهيئة مقارنة المحاضر الإدارية بالأذون المحالة عليها لمراقبة احترام الجهات المعنية للإجراءات القانونية عند تنفيذ عمليات النفاذ أو الاعتراض ومدى تقيّدها بالضوابط التي حددت في الاذون.

الفصل 36 :

يمكن للهيئة أن تطلب من الوكالة الفنية للاتصالات أو من السلطات المعنية مدها بمعطيات إضافية تهدف الى توضيح محتوى الاذن أو المحضر من شأنها أن تساعد على إجراء الرقابة.

الفصل 37:

يمكن للهيئة أن تتلقى الشكايات المتعلقة بالنفاذ الى قواعد البيانات والاعتراض على محتوى الاتصالات.

وتتولى الهيئة البحث في تلك الشكايات للتحقق من احترام الشروط والإجراءات القانونية دون المس بسرية عمليات النفاذ أو الإعتراض.

وفي صورة قيام شبهة على توفر جريمتي النفاذ أو الاعتراض غير المشروع أو مخالفة الاحكام المتعلقة بحماية المعطيات الشخصية تتولى الهيئة تحرير تقرير يحال على وكيل الجمهورية المختص ترابيا.

الفصل 38:

تحرر الهيئة تقريرا سنويا يتضمن استعراضا و تحليلا لعمليات المراقبة التي أنجزتها وتوصياتها يرفع الى رئيس المجلس التشريعي ورئيس الحكومة و رئيس الجمهورية.

ولا يتضمن التقرير معطيات شخصية.

ويمكن للسلط المنصوص عليها بالفقرة الأولى أن تأذن بنشر ملخصا تنفيذيا للعموم.

الفصل 39:

في صورة الإخلال بشروط أو إجراءات الاعتراض تقرر الهيئة بعد المداولة توجيه توصيات إلى رئيس الحكومة لتعديل إجراءات تنفيذ عملية نفاذ أو اعتراض محددة أو تعليقها عند الاقتضاء.

وفي صورة قيام شبهة على توفر جريمتي النفاذ أو الاعتراض غير المشروع أو مخالفة الاحكام المتعلقة بحماية المعطيات الشخصية تتولى الهيئة تحرير تقرير يحال على وكيل الجمهورية المختص ترابيا.

الفصل 40:

تتركب الهيئة من رئيس وعضوين كما يلي:

- قاض من الرتبة الثالثة، رئيسا.

- خبير في الشؤون الأمنية و العسكرية، عضوا
- خبير مهندس في تكنولوجيا الاتصال و المعلومات، عضوا

يتم إختيار أعضاء الهيئة من بين ثلاث شخصيات يقع إقتراحها من رئيس المجلس الأعلى للقضاء و المجلس الأعلى للمحكمة الإدارية بالنسبة لرئيس الهيئة و من رئيس الجمهورية بالنسبة للخبراء في الشؤون الأمنية والعسكرية و من رئيس المجلس التشريعي بالنسبة للخبراء في تكنولوجيا الاتصال والمعلومات

ويعين أعضاء الهيئة بأمر.

يمارس رئيس الهيئة مهامه بالتفرغ كامل الوقت لمدة خمس سنوات.

ويمارس عضوا الهيئة مهامهما بالتفرغ كامل الوقت لمدة أربع سنوات على أن يقع تجديد عضوية أحدهما بالتناوب كل ثلاثة سنوات وفقا لنفس الإجراءات.

الفصل 41:

يمارس أعضاء الهيئة مهامهم في كنف الاستقلالية والحياد وعلى أساس خدمة المصلحة العامة ولا يمكن عزلهم أو تعليق عضويتهم إلا في حالات العجز أو التغيب لأكثر من شهر دون مبرر أو خرق الواجبات المحمولة عليهم كارتكاب خطأ فادح أو تقصير في أداء واجبهم وذلك بموجب أمر معلل صادر عن رئيس الحكومة يخضع للطعن أمام المحكمة الإدارية طبقا لإجراءات قضاء مادة تجاوز السلطة.

وعليهم أن يجتنبوا أثناء أداء مهامهم كل ما من شأنه أن يؤثر على استقلاليتهم وحيادهم وأن يعلموا رئيس الحكومة بكل حالات تضارب المصالح أو كل تغيير يطرأ على وضعياتهم من شأنه الإخلال باستقلاليتهم.

الفصل 42:

لا يجوز لأعضاء الهيئة أن يتقاضوا بصورة مباشرة أو غير مباشرة أي أجرة باستثناء المستحقات الراجعة إليهم قبل مباشرة مهامهم على أن تراعى في ذلك حقوق الملكية الأدبية والفنية.

وتضبط بأمر المنح والامتيازات المخولة لأعضائها.

الفصل 43:

يحجر على أعضاء الهيئة وأعوانها إفشاء الأسرار المهنية المتعلقة بالوقائع والأعمال والمعلومات التي يطلعون عليها أو يحصل لهم العلم بها بمناسبة مباشرة مهامهم.
كما يحجر على أعضاء الهيئة إفشاء سرية مداولات الهيئة أو الإدلاء علنيا بأي تصريح له علاقة بالمعلومات المجمعة في عمليات الاعتراض التي باشرت مراقبتها.
ويستمر التحجير المشار إليه في الفقرتين المتقدمتين حتى بعد انتهاء مهام أعضاء الهيئة وأعوانها.

الباب الخامس

في دعم المجهود الدولي لمكافحة جرائم أنظمة المعلومات والاتصال

الفصل 44:

يمكن تتبع ومحاكمة كل من يرتكب خارج التراب التونسي إحدى الجرائم المنصوص عليها بهذا القانون في الصور التالية:

– إذا ارتكبت من قبل مواطن تونسي،

– إذا ارتكبت ضدّ أطراف أو مصالح تونسية،

– إذا ارتكبت ضدّ أطراف أو مصالح أجنبية من قبل أجنبي أو شخص عديم الجنسية يوجد محل إقامته المعتاد داخل التراب التونسي أو من قبل أجنبي أو شخص عديم الجنسية وجد بالتراب التونسي ولم تتوفر في شأنه شروط التسليم القانونية

الفصل 45:

تعمل السلطات المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصادق عليها أو طبق مبدأ المعاملة بالمثل قصد الإسراع بتبادل المعلومات بما من شأنه أن يكفل الإنذار المبكر **بجرائم أنظمة المعلومات والاتصال** وتفادي ارتكابها والمساعدة على التحقيق فيها وتتبع مرتكبيها.
ويتوقف التعاون المشار إليه بالفقرة المتقدمة على التزام الدولة الأجنبية المعنية بالحفاظ على سرية المعلومات المحالة إليها والتزامها بعدم إحالتها إلى طرف آخر أو استغلالها لأغراض أخرى غير مكافحة الجرائم المعنية بهذا القانون وزجرها.

مشروع قانون يتعلق بتنقيح بعض أحكام المجلة الجزائية

الفصل الأول: تلغى أحكام الفصل 172 من المجلة الجزائية وتعوض كما يلي:

الفصل 172 (جديد):
يعاقب بالسجن بقية العمر وبخطية قدرها ألف دينار كل موظف عمومي أو شبهه وكل عدل يرتكب في مباشرة وظيفه زورا من شأنه إحداث ضرر عام أو خاص وذلك بصنع كل أو بعض كتب أو عقد مكذوب أو بتغيير الحقيقة بأي وسلة كانت في كتب أو عقد يكون موضوعه أو يمكن أن ينجر عنه إثبات حق أو واقعة منتجة لآثار قانونية.

الفصل 2: تلغى أحكام الفصلان 199 مكرر و199 ثالثا من المجلة الجزائية.

مشروع قانون يتعلق
بمكافحة جرائم أنظمة المعلومات والاتصال

شرح الأسباب

شهدت السنوات الأخيرة تطورا هاما في مجال تكنولوجيات المعلومات والاتصال على الصعيدين العالمي والوطني لدرجة أثرت بصفة ملحوظة في مختلف مظاهر الحياة اليومية و طبعت بعمق نسق التبادل الاقتصادي و التواصل الاجتماعي و الإبداع الثقافي والفكري. وقد ساهمت في تحقيق هذه الآثار سهولة النفاذ إلى شبكات الاتصال بفضل ما شهدته البنية التحتية من تطور كبير وامتداد واسع وكذلك بفضل انتشار المعارف المتعلقة باستخدام هذه الوسائل لدى العموم.

وقد حظي قطاع تكنولوجيات المعلومات والاتصال بمكانة متميزة باعتباره أحد الروافد الأساسية في منظومة التنمية الشاملة، لكنه أفرز تحديات جديدة في مجال الأمن والسلامة المعلوماتية مرتبطة بالاعتداءات التي تهدف إلى النيل من أنظمة المعلومات والبيانات المعلوماتية أو استعمالها دون حق أو إلى المساس بحقوق الأشخاص أو النظام العام.

وقد تدخل المشرع التونسي منذ سنة 1999 لوضع إطار قانوني ضمن المجلة الجزائية لمكافحة الجرائم المتصلة بتكنولوجيات المعلومات والاتصال ، غير أن التطورات التي حصلت منذ ذلك التاريخ بينت أن هذا الإطار يشكو من بعض النقائص في مستوى الأحكام الموضوعية المتعلقة بالتجريم ومن فراغ في مستوى الأحكام الإجرائية.

كما شهد الإطار القانوني الدولي تطورا منذ اعتماد اتفاقية بيدابست لسنة 2001 وهي اتفاقية أوروبية المنشأ انضمت إليها عديد الدول المتطورة في هذا المجال وتعد حاليا الإطار المرجعي الدولي لمكافحة الجرائم المتصلة بتكنولوجيات المعلومات والاتصال. ويمكّن اعتماد المفاهيم الأساسية والمعايير المتعلقة بالتجريم والبحث والتحري الواردة في الاتفاقية من تدعيم إشعاع بلادنا على الصعيد الدولي في قطاع تكنولوجيات المعلومات والاتصال باعتبار أن التصدي للجرائم المتصلة بتلك التكنولوجيات يعد مؤشرا هاما في تقييم إنجازات القطاع.

ويتضمن مشروع القانون أحكاما عامة وأخرى تتعلق بالإجراءات و أحكاما موضوعية خاصة بالتجريم وأخيرا أحكاما خاصة بدعم التعاون الدولي.

1/ الأحكام العامة :

تتميز الجرائم المتصلة بتكنولوجيات المعلومات والاتصال بصبغتها الفنية المتطورة. وتؤثر هذه الخاصية في صياغة الأحكام الخاصة بها من خلال ضرورة اعتماد مصطلحات ومفاهيم مستحدثة ذات مدلول فني دقيق يعسر فهمها على غير المختصين والفنيين . لذلك اقترح مشروع القانون في باب الأحكام العامة تعريف أهم المفاهيم والمصطلحات الأساسية على غرار مفهوم نظام المعلومات وبيانات معلوماتية ومزود الخدمات لتيسير فهمها على غير المختصين وتجنب الاختلاف والتباين في تحديد معناها بما يضمن توحيد تأويل أحكام القانون وحسن تطبيقه.

2/ الأحكام الإجرائية :

ترتكب الجرائم المتصلة بتكنولوجيات المعلومات والاتصال في عالم افتراضي غير محسوس باستعمال تقنيات متطورة لذلك تتميز بصعوبة كشفها وإثباتها فأدلتها في أغلب الأحيان غير مادية وسريعة الاضمحلال وعسيرة الحفظ كما يتخفى مرتكبوها وراء هويات مصطنعة وغير حقيقية ويستعملون أساليب ذكية ومتشعبة يصعب كشفها وملاحقتها. وفي ضوء هذه الخصائص لا تكفي الأحكام العامة المتعلقة بمعاينة الجرائم وجمع أدلتها والبحث عن مرتكبيها لضمان التصدي الناجع للجرائم المتصلة بتكنولوجيات المعلومات و الاتصال التي تستوجب أحكاما خاصة تتلاءم مع طبيعتها وتزود السلطات المكلفة بمكافحتها بالوسائل و الإجراءات الكفيلة بكشفها وردعها.

وقد تضمن المشروع اقتراحا بتعزيز السلطات المكلفة بمعاينة الجرائم لتشمل ضابطة عدلية متخصصة من الأعوان التابعين للوزارة المكلفة بتكنولوجيات الاتصال إلى جانب اقتراح بعض الإجراءات الخاصة بجمع الأدلة الالكترونية مثل الإذن بالتمكين من البيانات المخزنة والنفاذ إلى أنظمة المعلومات وتفتيشها وحجز البيانات المعلوماتية والاعتراض الفوري لبيانات حركة الاتصالات.

وتعزيزا لقدرات الأعوان المكلفين بمعاينة الجرائم و ضمانا للعثور على أدلة مجدية في صورة ارتكاب جريمة حمّل مشروع القانون مزودي الخدمات عدة التزامات للمساهمة في مجهود مكافحة هذه الجرائم على غرار إلزامهم بواجب حفظ البيانات التي تمكن من تعريف المستعملين والأجهزة المستعملة ونوعية الخدمات المسداة وكذلك واجب المساعدة على اعتراض بيانات حركة الاتصالات ومحتواها.

ويعد إقرار هذه الإجراءات الخاصة ضروريا للوقاية من هذه الجرائم وردعها لكن ذلك لم يمنع من إحاطتها بقواعد وضوابط دقيقة لضمان عدم المساس بالحقوق والحريات الفردية كما أنها لا تمارس إلا في حالات محددة وتحت إشراف قضائي مباشر.

ولدعم نجاعة تلك الإجراءات اقترح المشروع تجريم الإخلال بواجب حفظ البيانات وإعاقة سير البحث بإعدام بيانات أو إخفائها قبل حجزها وكذلك انتهاك سرية الإجراءات المتعلقة بجمع الأدلة أو إفشاء البيانات المتحصل عليها .

3/ **الأحكام الموضوعية :**

تهدف الأحكام الموضوعية إلى توسيع نطاق التجريم ليشمل أفعالا جديدة غير معاقب عنها قصد التصدي للحالات المسجلة والتوقي من انتشارها، فأضيفت إلى الجرائم المتعلقة بالاعتداء على أنظمة المعلومات والبيانات المعلوماتية جريمة الاعتراض غير المشروع وجريمة إساءة استخدام الأجهزة والبيانات المعلوماتية. كما أضيفت إلى الجرائم المرتكبة بواسطة أنظمة أو بيانات معلوماتية جريمة الاحتيال المعلوماتي. وأخيرا تضمن المشروع تجريم مجموعة من الأفعال المتعلقة بالمحتوى المعلوماتي غير المشروع .

كما تضمنت الأحكام الموضوعية تعديلا في تجريم الأفعال التي يشملها الإطار القانوني الحالي لتوضيح أركانها بدقة و ملاءمتها للمعايير الدولية و شمل التعديل جرائم النفاذ غير المشروع و الاعتداء على أنظمة المعلومات والاعتداء على البيانات المعلوماتية فأضحت كل جريمة منها مستقلة لها أركانها الخاصة بما مكّن من توسيع نطاق التجريم ليشمل أفعالا جديدة لم يكن من الممكن تتبعها في نطاق الأحكام النافذة حاليا.

وضمانا لتكامل الإطار القانوني لمكافحة الجرائم المتصلة بتكنولوجيات المعلومات والاتصال وقع إدراج جريمة التدليس المعلوماتي في هذا المشروع مع اقتراح إلغائها من المجلة الجزائية في إطار مشروع قانون مستقل.

4/ **أحكام خاصة بالتعاون الدولي** :

من أهم خصائص الجرائم المتصلة بتكنولوجيات المعلومات والاتصال صبغتها العابرة للحدود الوطنية باعتبارها ترتكب ضد أنظمة معلومات أو بواسطتها مرتبطة في ما بينها بشبكات اتصال ذات امتداد عالمي. وتحتم هذه الخاصية تنسيق الجهود في جميع الدول للإنذار المبكر من هذه الجرائم و كشفها وردعها. وقد تضمن مشروع القانون أحكاما خاصة بتيسير التعاون الدولي عن طريق الإسراع بتبادل المعلومات قصد الوقاية من هذه الجرائم و كشفها. كما أقر المشروع توسيع اختصاص المحاكم للنظر في الجرائم المرتكبة خارج التراب التونسي.

تلك هي أهم أسباب مشروع القانون