**Faculty of law and political sciences**

**Department of law**

**Master 2/ Electronic administration & Digital services**

**Texts of English module**

**الفئة المستهدفة: طلبة السنة الثانية ماستر تخصص الادارة الالكترونية والخدمات المرفقية**

**من اعداد الاستاذة: زراري حبيبة**

**السنة الجامعية: 2022/ 2023**

**Master2/ Electronic Administration&Digital services**

***Text N° :01***

***The Electronic Trade***

 The technological developments that have marked the current time are not without throwing their impacts on multilateral trade activity. Several changes are noted in contemporary business practices. The advent of electronic intermediaries is undoubtedly the fact that marked the commercial practice of the third millennium. This gave rise to what is called e-commerce. A commercial genre that differs from traditional trade.

The electronic commerce or e-commerce is a term for any type of business, or commercial transaction that involves the transfer of information across the Internet. It covers a range of different types of businesses, retail sites, business exchanges trading goods and services between corporation. It is currently one of the most important aspects of the Internet.

 E-commerce allows consumers to electronically exchange goods and services with no barriers of time or distance. Electronic commerce has expanded rapidly over the past five years and is predicted to continue at this rate, or even accelerate. In the near future the boundaries between "conventional" and "electronic" commerce will become increasingly blurred as more businesses move sections of their operations into the Internet.

**The Electronic signature**

 Technological development and the entry of electronic commerce in financial transactions, is an urgent need to find a Safe and quick use in transaction documentation Electronic. The traditional way can delay or hinder the contracted between the parties, that is why electronic signature replaces the Traditional signature. The digital signature is a mechanism for guaranteeing the integrity of an electronic document and authenticate the author to document of transaction that are made over the Internet, the Electronic signature ensures the identity of the holders of this signature and their consent, and the authenticity of the document that is exchanged between the Parties, so that it is against the law any fraud, either with the consent of the owner or otherwise, despite the reliability of the electronic signature, most of the Risk such as piracy, which prevent the use of this signature which requires technical mechanisms, and legal measures for the secure and protect it at the national and international level.

**The proof in electronic commerce**

All along the stages of the commercial operation (negotiations, conclusion, proof….)E-commerce presents a peculiarity that is distinct from what is known in traditional commerce. The evidence is considered as an essential link in in e-commerce. The conclusion of commercial leases in a virtual environment, marked by the absence of paper media that are replaced by electronic documents, or the electronic signature substituted for the Handwritten Signature accentuates the importance of this evidence.

***التجارة الالكترونية***

إن التطورات التكنولوجية التي ميزت الوقت الحالي لا تخلو من إلقاء آثارها على النشاط التجاري متعدد الأطراف. حيث تم تسجيل العديد من التحولات على الممارسات التجارية المعاصرة، فظهور الوسائط الالكترونية هو بلاشك الحقيقة التي ميزت الممارسة التجارية في الألفية الثالثة وأدى هذا إلى ظهور ما يسمى التجارة الإلكترونية، ذلك النوع التجاري الذي يختلف عن التجارة التقليدية.

إن التجارة الإلكترونية مصطلح لأي نوع من الأعمال، أو المعاملات التجارية التي تنطوي على نقل المعلومات عبرالإنترنت. وهي تغطي مجموعة من الأنواع المختلفة من الشركات، مواقع البيع بالتجزئة، إلى أعمال المبادلات التجارية للسلع والخدمات التجارية بين الشركات. وتشكل حاليا أحد أهم جوانب الإنترنت.

تتيح التجارة الإلكترونية للمستهلكين تبادلا للسلع والخدمات إلكترونيا دون حواجز زمنية أو مسافات. وقد توسعت التجارة الإلكترونية بسرعة خلال السنوات الخمس الماضية ومن المتوقع أن تستمر بهذا المعدل أو حتى تتسارع في المستقبل القريب، ستصبح الحدود بين التجارة التقليدية والإلكترونية غير واضحة بشكل متزايد مع قيام المزيد من الشركات بنقل أقسام من عملياتها إلى الإنترنت.

**التوقيع الإلكتروني**

إن التطور التكنولوجي ودخول التجارة الإلكترونية في المعاملات المالية ضرورة ملحة لإيجاد استخدام آمن وسريع في توثيق المعاملات الإلكترونية. فالطريقة التقليدية يمكن أن تؤخر أو تعيق التعاقد بين الطرفين، لهذا السبب حل التوقيع الإلكتروني محل التوقيع التقليدي.إذ يعد التوقيع الرقمي آلية لضمان صحة (سلامة، نزاهة) الوثيقة الإلكترونية وتصديق صاحبها لوثيقة المعاملة التي تتم عبر الإنترنت، ويضمن التوقيع الإلكتروني هوية حاملي هذا التوقيع وموافقتهم، وصحة الوثيقة التي يتم تبادلها بين الطرفين ، بحيث يكون مخالفا للقانون أي تزوير، سواء بموافقة صاحبه أو دون ذلك، رغم موثوقية (مصداقية) التوقيع الإلكتروني، فإن معظم المخاطر مثل القرصنة تمنع استخدام هذا التوقيع الذي يتطلب آليات فنية وإجراءات قانونية لتأمينه وحمايته على المستوى الوطني والدولي.

**الإثبات في التجارة الإلكترونية**

على طول مراحل العمليات التجارية (المفاوضات، الإبرام، الإثبات….) تطرح التجارة الإلكترونية خصوصية مميزة تختلف عما هو معروف في التجارة التقليدية، إذ يعتبر الدليل حلقة أساسية في التجارة الإلكترونية، وإن إبرام عقود الإيجار التجارية في بيئة افتراضية تتميز بغياب الوسائط الورقية التي يتم استبدالها بمستندات إلكترونية، أو التوقيع الإلكتروني الذي يحل محل التوقيع الخطي ما يبرز أهمية هذا الدليل.

**Master2/ Electronic Administration&Digital services**

***Text N° :02***

ICT as a tool for citizen participation in anti-corruption efforts

 Information and communication technology (ICT) has become a very useful tool for fighting corruption. Of course, ICT-based social media has added a new dimension to the fight against corruption as information can find its way around the world in a matter of minutes and viral pictures or videos taken by citizen journalists can be used as evidence of corruption. In addition, these videos and images may be a catalyst for governmental action and can be used by the international community to apply pressure on States. The Internet gives a global dimension to the work of local CSOs and also enables collaborative investigative journalism. Some of the ways in which ICT is useful in the fight against corruption, and in particular in enhancing citizen participation in anti-corruption efforts, are:

**Sharing information**: Technology can be used to provide a platform for sharing information on cases of corruption, which can raise awareness of these cases and may act as a deterrent. For instance, platforms such as [I Paid a Bribe](http://www.ipaidabribe.com/) in India provide crowdsourced information on demand bribery in different contexts. evidence suggests that those demanding bribes in areas where these platforms are used become more reluctant for fear of being identified on these platforms .

**Automation and digitization of government processes and services, including blockchain-enabled platforms**: Technology has been used to automate government processes and reduce the face time public officials in certain positions have with the public. Automation may limit the discretion of public officials, increase transparency and make it more difficult for corrupt transactions to be effected. In addition, automation and digitization may provide a verifiable audit trail that makes it harder to hide corrupt transactions. This is one of the benefits that the blockchain technology is expected to provide. The technology became popular because of its ability to transfer data in a safe, tamper-proof and transparent manner. The data is stored in many devices rather than on one centralized server, which in combination with heavy-duty encryption, makes the system impossible to be hacked. On the other hand, this encryption does not allow the changing or deletion of information once it enters the system. Moreover, the blockchain's open source code makes the information publicly available and easy to trace at any time. In particular, the provision of government services on a blockchain-enabled platform could prevent fraud. The automation and digitization of government services ultimately facilitates access to information, which makes it easier for citizens to understand and engage with relevant processes - thus enhancing their ability to monitor the transactions and detect any irregularities.

**Big data analytics**: ICT enables citizens and civil society actors to utilize big data in a way that can assist in targeted change and reforms and in the understanding of trends and patterns relevant to anti-corruption enforcement.). Data sets like financial disclosure, beneficial ownership, company data, financial intelligence data, tax authority data and procurement data could be analysed to provide patterns and evidence of procurement fraud or other acts of corruption.

**Legal terms**

|  |  |
| --- | --- |
| مشاركة المواطنين في جهود مكافحة الفساد | citizen participation in anti-corruption efforts |
| مكافحة الفساد | fighting corruption |
| العمل الحكومي | governmental action |
| المجتمع الدولي  | international community |
| الدولة  | State  |
| منظمات المجتمع المدني  | CSOs  |
| الصحافة الاستقصائية التعاونية | collaborative investigative journalism. |
| تعزيز | enhancing  |
| رادع | A detterent  |
| اتمتتة ورقمنة العمليات والخدمات الحكومية  | Automation and digitization of government processes and services |
| السلطة التقديرية للموظفين الحكوميين  | the discretion of public officials |
| الشفافية  | Transparency |
| مسار تدقيق يمكن التحقق منه | verifiable audit trail |
| القدرة  | Ability |
| الخدمات الحكومية | government services |
| النفاذ الى المعلومة | Acess to information |
| تعزيز القدرة على رقابة المعاملات  | enhancing the ability to monitor the transactions  |
| الكشف عن المخالفات  | To detect irregularities  |
| الاصلاحات  | Reforms |
| الاحتيال في الصفقات  | Procurment fraud |
| يمكن  | To enable |

***تكنولوجيا الاعلام والاتصال كوسيلة لمشاركة المواطنين في جهود مكافحة الفساد***

أصبحت تكنولوجيا المعلومات والاتصالات أداة مفيدة للغاية في مكافحة الفساد. حيث أضافت وسائل التواصل الاجتماعي القائمة على تكنولوجيا المعلومات والاتصالات بعدًا جديدًا لمكافحة الفساد، حيث يمكن للمعلومات أن تجد طريقها حول العالم في غضون دقائق، ويمكن استخدام الصور أو مقاطع الفيديو الحية التي يلتقطها المواطنون الصحفيون كدليل على الفساد.

إضافة إلى ذلك، قد تكون مقاطع الفيديو والصور هذه حافزًا للعمل الحكومي ويمكن للمجتمع الدولي استخدامها للضغط على الدول. تعطي الإنترنت بُعدًا عالميًا لعمل منظمات المجتمع المدني المحلية كما تتيح أيضًا ما يعرف بالصحافة الاستقصائية التعاونية.

ومن الطرق التي تساهم من خلالها تكنولوجيا المعلومات والاتصالات في مكافحة الفساد لا سيما في تعزيز مشاركة المواطنين في جهود مكافحة الفساد نذكر مايلي:

1/مشاركة المعلومات: يمكن استخدام التكنولوجيا لتوفير منصة لتبادل المعلومات حول حالات الفساد، والتي يمكن أن تزيد من الوعي بهذه الحالات وقد تكون بمثابة رادع فعلى سبيل المثال، توفر منصات مثل دفعت رشوة في الهند معلومات عن التعهيد الجماعي بشأن الطلب على الرشوة في سياقات مختلفة.

كما تشير الأدلة إلى أن أولئك الذين يطلبون الرشاوى في المناطق التي تُستخدم فيها هذه المنصات يصبحون أكثر ترددًا خوفًا من التعرف عليهم على هذه المنصات.

2/أتمتة العمليات والخدمات الحكومية ورقمنتها، بما في ذلك المنصات التي تدعم تقنية blockchain: يتم استخدام التكنولوجيا لأتمتة العمليات الحكومية وتقليل وقت مواجهة المسؤولين الحكوميين في بعض

 المناصب مع الجمهور، فقد تحد الأتمتة من السلطة التقديرية للموظفين العموميين، وتزيد من الشفافية وتجعل من الصعب إجراء المعاملات الفاسدة. بالإضافة إلى ذلك، قد توفر الأتمتة والرقمنة مسار تدقيق يمكن التحقق منه مما يجعل من الصعب إخفاء المعاملات الفاسدة.

هذه إحدى الفوائد التي من المتوقع أن توفرها تقنية ( سلسلة الكتل) blockchain، حيث أصبحت هذه التكنولوجيا أكثر شيوعا بسبب قدرتها على نقل البيانات بطريقة آمنة ومقاومة للعبث وشفافيتهاـ إذ يتم تخزين البيانات في العديد من الأجهزة بدلاً من خادم مركزي واحد، مما يجعل من المستحيل اختراق النظام إلى جانب التشفير القوي. ومن ناحية أخرى، لا يسمح هذا التشفير بتغيير أو حذف المعلومات بمجرد دخولها إلى النظام. علاوة على ذلك ، فإن شفرة المصدر المفتوح blockchain تجعل المعلومات متاحة للجمهور ويسهل تتبعها في أي وقت. وعلى وجه الخصوص، يمكن أن يؤدي توفير الخدمات الحكومية على منصة تدعم تقنية blockchain إلى منع الاحتيال.

 تسهل أتمتة الخدمات الحكومية ورقمنتها الوصول إلى المعلومات، مما يسهل على المواطنين فهم العمليات ذات الصلة والتعامل معها - وبالتالي تعزيز قدرتهم على مراقبة المعاملات واكتشاف أي مخالفات.

3/تحليلات البيانات الضخمة: تُمكّن تكنولوجيا المعلومات والاتصالات المواطنين وفواعل المجتمع المدني من استخدام البيانات الضخمة بطريقة يمكن أن تساعد في التغيير والإصلاحات المنشودة وفي فهم الاتجاهات والأنماط ذات الصلة بإنفاذ مكافحة الفساد). يمكن تحليل مجموعات البيانات مثل الافصاح المالي والملكية وبيانات الشركة وبيانات الذكاء المالي وبيانات مصلحة الضرائب وبيانات الصفقات لتوفير أنماط وأدلة على الاحتيال في الصفقات أو أعمال الفساد الأخرى.

**Master2/ Electronic Administration&Digital services**

***Text N° :03***

**E- payment system**

 An **e-commerce payment system** (or an **electronic payment system**) facilitates the acceptance of electronic [payment](https://en.wikipedia.org/wiki/Payment) for [online transactions](https://en.wikipedia.org/wiki/E-commerce). Also known as a subcomponent of [electronic data interchange](https://en.wikipedia.org/wiki/Electronic_data_interchange) (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

[Credit cards](https://en.wikipedia.org/wiki/Credit_card) remain the most common forms of payment for e-commerce transactions. As of 2008, almost 90% of online retail transactions were made with this payment type. It is difficult for an online retailer to operate without supporting credit and debit cards due to their widespread use. Online merchants must comply with stringent rules stipulated by the credit and debit card issuers (e.g. [Visa](https://en.wikipedia.org/wiki/Visa_Inc.) and [Mastercard](https://en.wikipedia.org/wiki/Mastercard)) in accordance with [bank](https://en.wikipedia.org/wiki/Bank_regulation) and [financial regulation](https://en.wikipedia.org/wiki/Financial_regulation) in the countries where the debit/credit service conducts business. For the vast majority of payment systems accessible on the public Internet, baseline [authentication](https://en.wikipedia.org/wiki/Electronic_authentication) (of the financial institution on the receiving end), [data integrity](https://en.wikipedia.org/wiki/Data_integrity), and [confidentiality](https://en.wikipedia.org/wiki/Privacy) of the electronic information exchanged over the public network involves obtaining a certificate from an authorized [certificate authority](https://en.wikipedia.org/wiki/Certificate_authority) who provides [public-key infrastructure](https://en.wikipedia.org/wiki/Public-key_infrastructure) .

Despite widespread use, there are still many countries such as China and India that have some problems to overcome in regard to credit card security. Increased security measures include use of the [card verification number](https://en.wikipedia.org/wiki/Card_security_code) (CVN) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank. There are companies that specialize in financial transaction over the Internet, such as [Stripe](https://en.wikipedia.org/wiki/Stripe_%28company%29) for credit cards processing, Smartpay for direct online bank payments and [PayPal](https://en.wikipedia.org/wiki/PayPal) for alternative payment methods at checkout. Many of the mediaries permit consumers to establish an account quickly, and to transfer funds between their on-line accounts and traditional [bank accounts](https://en.wikipedia.org/wiki/Bank_account), typically via [automated clearing house](https://en.wikipedia.org/wiki/Automated_clearing_house) (ACH) transactions

**Methodes of online payment :** There are varied types of electronic payment methods such as online credit card transactions, e-wallets, e-cash and wireless payment system. Credit cards constitute a popular method of online payment but can be expensive for the merchant to accept because of transaction fees primarily. Debit cards constitute an excellent alternative with similar security but usually much cheaper charges. Besides card-based payments, [alternative payment](https://en.wikipedia.org/wiki/Alternative_payment) methods have emerged and sometimes even claimed market leadership.

**Bank payments**: This is a system that does not involve any sort of physical card. It is used by customers who have accounts enabled with [Internet banking](https://en.wikipedia.org/wiki/Internet_Banking). Instead of entering card details on the purchaser's site, in this system the payment gateway allows one to specify which bank they wish to pay from. Then the user is redirected to the bank's website, where one can authenticate oneself and then approve the payment. It is typically seen as being safer than using credit cards, as it is much more difficult for hackers to gain login credentials compared to credit card numbers. For many e- Commerce merchants, offering an option for customers to pay with the cash in their bank account reduces cart abandonment as it enables a way to complete a transaction without credit cards.

**Mobile money wallets**: In some developing countries, many people do not have access to banking facilities, especially in tier II and tier III cities. Taking the example of India, there are more mobile phone users than there are people with active bank accounts. Telecom operators, in such locations, have started offering mobile money wallets which allow adding funds easily through their existing mobile subscription number, by visiting physical recharge points close to their homes and offices and converting their cash into mobile wallet currency. This can be used for online transaction and e- Commerce purchases.

**Legal terms**

|  |  |
| --- | --- |
| e- payment system | نظام الدفع الالكتروني  |
| e- commerce payment system | نظام الدفع في التجارة الالكترونية |
| Online transactions  | المعاملات الخطية ( الالكترونية) |
| Internet- based shopping and banking  | التسوق والخدمات المصرفية عبر الانترنت |
| Credit and debit cards  | بطاقات الخصم والائتمان |
| Bank and financial regulation  | اللوائح والتنظيمات المصرفية والمالية |
| Baseline authentication | المصادقة الاساسية |
| Fiannacial institution | المؤسسة المالية |
| Data intergrity | نزاهة البيانات  |
| Confidentiality | السرية |
| Authorized certificate authority | سلطة المصادقة المختصة |
| Security measures | الاجراءات (التدابير) الامنية |
| financial transaction | المعاملة المالية |
| Alternative payment methodes  | طرق الدفع البديلة |
| Online accounts  | الحسابات الخطية  |
| Internet banking  | الخدمات المصرفية عبر الانترنت |
| To approve  | يوافق – الموافقة  |

**نظام الدفع الالكتروني**

يسهل نظام الدفع للتجارة الإلكترونية (أو نظام الدفع الإلكتروني) الدفع الإلكتروني للمعاملات عبر الإنترنت. كما يشكل مكونا فرعيا لتبادل البيانات الإلكترونية (EDI)، وبسبب الاستخدام الواسع النطاق للتسوق والخدمات المصرفية عبر الإنترنت أصبحت أنظمة الدفع للتجارة الإلكترونية تعرف انتشارا متزايدا.

تظل بطاقات الائتمان هي أكثر طرق الدفع شيوعًا لمعاملات التجارة الإلكترونية، اعتبارًا من عام 2008، تم إجراء ما يقرب من 90٪ من معاملات البيع بالتجزئة عبر الإنترنت باستخدام هذا النوع من الدفع.إذ يصعب على باعة التجزئة عبر الإنترنت القيام بنشاطهم دون الاعتماد على بطاقات الائتمان والخصم نظرًا لاستخدامها على نطاق واسع.

 يجب على التجار عبر الإنترنت الالتزام بالقواعد الصارمة المنصوص عليها من قبل مصدري بطاقات الائتمان والخصم (مثل Visa و Mastercard) وفقًا للوائح المصرفية والمالية في البلدان التي تمارس فيها خدمة الخصم / الائتمان أعمالها.

بالنسبة للغالبية العظمى من أنظمة الدفع التي يمكن الوصول إليها على الإنترنت العام، فإن المصادقة الأساسية (للمؤسسة المالية على الطرف المتلقي)، سلامة البيانات، وسرية المعلومات الإلكترونية التي يتم تبادلها عبر الشبكة العامة يجب أن تتضمن الحصول على شهادة من سلطة تصديق معتمدة والتي توفر البنية التحتية الهامة.

على الرغم من هذا الاستخدام الواسع النطاق لا تزال العديد من البلدان مثل الصين والهند لديها بعض المشاكل يجب التغلب عليها فيما يتعلق بأمان بطاقة الائتمان. حيث تشمل الإجراءات الأمنية المتزايدة استخدام رقم التحقق من البطاقة (CVN) الذي يكشف عن الاحتيال من خلال مقارنة رقم التحقق المطبوع على شريط التوقيع على ظهر البطاقة بالمعلومات الموجودة في الملف لدى البنك الذي أصدر البطاقة.

هناك شركات متخصصة في المعاملات المالية عبر الإنترنت، مثل Stripe لمعالجة بطاقات الائتمان و Smartpay للمدفوعات المصرفية المباشرة عبر الإنترنت و PayPal لطرق الدفع البديلة. يسمح العديد من الوسطاء للمستهلكين بإنشاء حسابات بسرعة، وتحويل الأموال بين حساباتهم عبر الإنترنت والحسابات المصرفية التقليدية عادةً عبر معاملات غرفة المقاصة الآلية (ACH).

**طرق الدفع عبر الإنترنت**

هناك أنواع متنوعة من طرق الدفع الإلكترونية مثل معاملات بطاقات الائتمان عبر الإنترنت والمحافظ الإلكترونية والنقد الإلكتروني ونظام الدفع اللاسلكي، حيث تشكل بطاقات الائتمان طريقة شائعة للدفع عبر الإنترنت، ولكنها قد تكون مكلفة للتاجر بسبب رسوم المعاملات في المقام الأول، أما بطاقات الخصم فتشكل بديلاً ممتازًا وبأمان مماثل ولكن عادةً ما تكون رسومها أرخص بكثي، إلى جانب المدفوعات القائمة على البطاقات، ظهرت طرق دفع بديلة واعتلت الريادة أحيانا في السوق.

**المدفوعات المصرفية**

هذا النظام لا يتضمن أي نوع من البطاقات، يتم استخدامه من قبل العملاء الذين لديهم حسابات ممكّنة مع الخدمات المصرفية عبر الإنترنت. فبدلاً من إدخال تفاصيل البطاقة على موقع المشتري تسمح بوابة الدفع في هذا النظام للشخص بتحديد البنك الذي يرغب في الدفع منه. ثم يتم إعادة توجيه المستخدم إلى الموقع الإلكتروني للبنك، حيث يمكنه المصادقة مرة واحدة ثم الموافقة على الدفع.

يُنظر إلى هذا النوع من الدفع عادةً على أنه أكثر أمانًا من استخدام بطاقات الائتمان، حيث يصعب على المتسللين الحصول على بيانات اعتماد تسجيل الدخول مقارنة بأرقام بطاقات الائتمان. فبالنسبة للعديد من تجار التجارة الإلكترونية فإن تقديم خيار للعملاء للدفع نقدًا في حسابهم المصرفي يقلل من التخلي عن سلة التسوق لأنه يتيح طريقة لإكمال معاملة بدون بطاقات ائتمان.

**محافظ النقود المتنقلة**

في بعض البلدان النامية، لا يستطيع الكثير من الناس الوصول إلى التسهيلات المصرفية، فمثلا في الهند يوجد عدد أكبر من مستخدمي الهاتف المحمول من الأشخاص الذين لديهم حسابات بنكية نشطة. حيث بدأ متعاملي الاتصالات في مثل هذه المواقع في تقديم محافظ النقود عبر الهاتف المحمول والتي تسمح بإضافة الأموال بسهولة من خلال ارقام اشتراكاتهم الحالية في الهاتف المحمول، من خلال زيارة نقاط إعادة الشحن الفعلية بالقرب من منازلهم ومكاتبهم وتحويل أموالهم إلى محفظة النقود المتنقلة، وهو ما يمكن استخدامه في المعاملات عبر الإنترنت ومشتريات التجارة الإلكترونية.

**Master2/ Electronic Administration&Digital services**

***Text N° 04***

***E- Governance***

 **Definitions of E-Governance**: The concept of e-governance started to appear in the early 1990 among American scholars. The prevailing ideas were ―e-government‖, ―electronic government‖, and ―people online instead of in line. In that time, there were emergence of Internet and developments in processing capacity and data storage. This fact has significantly altered the environment for ICT use across society and in government. UNESCO (2005) defines e-governance as the performance of governance via the electronic medium in order to facilitate an efficient, speedy and transparent process of disseminating information to the public, and other agencies, and for performing government administration activities. E-governance is a concept larger than the concept of e-government since it can bring about a change in the way how citizens relate to government and to each other. Indeed, e-governance embodies new concepts of citizenship, both in terms of citizen needs and responsibilities. Its objective is to engage, enable and empower the citizen. Electronic Governance can be also defined as the application of technology by government to transform itself and its interactions with customers, in order to create impact on the society.

 The definition clearly identifies five dimensions of EGOV: government, technology, interaction, customers and society. Under each dimension, we list a number of defining elements like : mission, role, values, operations, services, institutions, inspection and enforcement under the government dimension. The five dimensions are meant to cover the whole EGOV space but the list of elements under each dimension is open-ended.

It has been proven from the concept of e-governance that it is a powerful means of public service in the present era. Some of its features can be found by observing the functioning of e-governance.

1. **De-bureaucratization**: Due to e-governance, the gap between the people and the government in all the services of the government is narrowing and the dependence of the people on the bureaucracy is also greatly reduced.

 2. E-**Services**: Its main feature is the provision of services through the Internet.

**3. International Services**: through e-governance, all the essential services can be delivered to the citizens who are living outside of their country for job purposes or any other reasons.

**4. Enhancing the right to express to the citizens**: Using the means of e-governance anyone can share their views with the government on any bill or act or decision taken by the government.

5**. Economic Development**: With the introduction of e-governance, various information like import-export, registration of companies, investment situations, etc. are available through the internet. As a result, time is saved, procrastination decreases, and economic dynamism increases.

6. **Reduce inequality**: using e-governance tools everyone can gather information and empower themselves. In this globalized world, knowledge is power, and means of egovernance empower us by providing relevant information at minimal cost, effort, and time.

**Legal terms** :

|  |  |
| --- | --- |
| E- Governance | الحوكمة الالكترونية |
| ICT (information and communication technology) | تكنولوجيا الاعلام والاتصال  |
| the performance of governance electronic medium وسيط الكتروني  | آداء الحوكمة  |
| an efficient, speedy and transparent process of disseminating information,  | عملية فعالة، سريعة وشفافة في نشر المعلومة  |
| the public | الجمهور |
| The agencies  | الهيئات ( الوكالات) |
| performing government administration activities | تحسين نشاطات ادارات الحكومة  |
| e-government | الحكومة الالكترونية  |
| Citizens | المواطنين  |
| Citizenship | المواطنة  |
| Responsibilities | المسؤوليات  |
| to engage | اشراك  |
| To enable and empower | يمكن ( تمكين) |
|  mission, role, values,  | مهمة، دور، قيم |
| operations, services, institutions | عمليات، خدمات، مؤسسات  |
|  inspection and enforcement  | التفتيش والانفاذ |
| Public service | المرفق العمومي |
| the functioning of e-governance.  | سير وعمل الحوكمة |
| De-bureaucratization | القضاء على البيروقراطية |
| e-services  | الخدمات الالكترونية |
| International services  | الخدمات الدولية  |
| Enhancing the right to express to the citizens | تعزيز حق المواطنين في التعبير |
| bill or act or decision | وثيقة ( مشروع قانون)، تصرف او قرار  |
| Economic development | التنمية الاقتصادية  |
| investment situations | وضعيات الاستثمار  |
| Reduce of inequality | تخفيض اللامساواة  |
| Globalized world | العالم المعولم  |
| providing information | توفير المعلومات  |

**الحوكمة الالكترونية:**

لقد بدأ مفهوم الحوكمة الالكترونية في الظهور في بداية التسعينات في الأوساط الأكاديمية الأمريكية، حيث كانت الأفكار السائدة تتمحور حول الحكم الالكتروني، الناس عبر الخط بدلا من الناس على الخط ( الطابور)، حيث باتت ضرورة الانترنت ومختلف التطورات في معالجة القدرات وتخزين البيانات أمرا ضروريا.

وقد كان لهذا الوقع تغيير كبير في بيئة استعمال تكنولوجيا الإعلام والاتصال من خلال المجتمع والحكومة، إذ عرفت منظمة اليونسيكو الحوكمة الالكترونية بأنها أداء للحوكمة من خلال الوسائط الالكترونية بهدف تسهيل عملية معالجة ونشر معلومة فعالة ، سريعة وشفافة للجمهور ولهيئات أخرى ولتحسين نشاطات الإدارة الحكومية.

إن مفهوم الحوكمة المحلية أوسع من مفهوم الحكومة الالكترونية بما أنها تنصب على التحول في الطريقة التي تربط المواطنين بالحكومة.

في الواقع، تجسد الحوكمة الالكترونية العديد من مفاهيم المواطنة سواء من حيث احتياجات المواطنين ومسؤولياتهم، حيث تهدف إلى إشراك المواطنين وتمكينهم.

يمكن تعريف الحوكمة الالكترونية بانها تطبيق لتكنولوجيا المعلومات من طرف الحكومة لتحول نفسها وتفاعلاتها مع عملائها بهدف التأثير على المجتمع.

يحدد هذا التعريف بوضوح الابعاد الخمسة للحوكمة الالكترونية: الحكومة، التكنولوجيا، التفاعل، العملاء والمجتمع، وكل بعد يتضمن مجموعة من العناصر المحددة على غرار: المهمة، الدور، القيم، العمليات، الخدمات، المؤسسات، التفتيش والانفاذ ضمن بعد الحكومة.

ويكمن الهدف من هذه الابعاد في تغطية الفضاء الشامل للحكومة الالكترونية لتبقى بذلك قائمة العناصر مفتوحة ضمن كل بعد.

فمن خلال مفهوم الحوكمة الالكترونية التي هي وسيلة قوية لتقديم الخدمات العمومية في وقتنا الحالي، إلا أن بعض ملامحها تتضح من خلال ملاحظة طريقة عمل وسير الحوكمة الالكترونية ومن اهدافها نذكر:

**القضاء على البيروقراطية**: حيث تضيق الفجوة بين الأفراد والحكومة على مستوى كل خدمات الحكومة، كما أن اعتماد الناس على البيروقرطية سوف يتناقص بشكل كبير.

**الخدمات الالكترونية**: وهي الامتياز الرئيسي في تقديم الخدمات من خلال الانترنت.

الخدمات الدولية: من خلال الحوكمة الالكترونية يمكن تقديم كل الخدمات الاساسية للمواطنين المتواجدين خارج دولهم لاسباب تتعلق بالشغل أو أخرى.

**تعزيز حق المواطنين في التعبير**: وذلك باستخدام وسائل الحوكمة الاكترونية، حيث يشاركون اراءهم مع الحكومة حول أي مشروع قانون، وثيقة أو تصرف أو قرار يمكن أن تتخذه هذه الاخيرة.

التنمية الاقتصادية: فبإدخال الحوكمة الالكترونية، اصبحت العديد من المعلومات حول الاستراد والتصدير، تسجيل الشركات، وضعيات الاستثمار.... متاحة عبر الانترنت وبالنتيجة اختصار للزمان.

**تخفيف اللامساواة**: ان إستعمال وسائل الحوكمة الالكترونية يمكن الافراد من جمع المعلومات وتمكين أنفسهم في هذا العالم المعولم، الذي أصبحت فيه المعرفة هي القوة وأن وسائل الحوكمة الالكترونية ستمكن منخلال توفير المعلومات المتعلقة ، بأقل تكلفة واقل جهد ووقت.

**Master2/ Electronic Administration&Digital services**

***Text N° :05***

**E-COVERNANCE (Part 2)**

**Principles and Objectives of E-governance**

The principles of e-governance are to:

-Build services with citizen choices in mind

- Increase government accessibility;

-Foster social inclusion;

-Disseminate information in a responsible fashion

- Use taxpayers resources effectively and efficiently

**Objectives of e-governance**.

objectives of e-governance include the following:

-To ensure transparency in the workings of government;

-To ensure greater efficiency, objectivity, accountability and speed in providing services and information to the public;

-To provide qualitative and cost-effective services;

-To provide a single window for all government services;

-To evolve responsive administration;

-To provide a friendly, speedier and efficient interface; and

-To eliminate the middlemen

**Domains of e-governance**

There are three main domains of e-governance:

E-administration: improving government processes

E-services: connecting individual citizens with their government

E-society: building interactions with and within civil society.

- **E-administration** – the main purpose of e-administration is to improve the internal working of the public sector by cutting process costs, managing process performance,

creating strategic connections within government bodies, and creating empowerment. Shortening the lead time for passport application from two weeks to one day is an example of e-administration.

- **E-service** initiative focus mainly on improving the relationship between the government and its citizens by increasing the information flow between them – which notably, involves two- way communication – and improving the service levels of government towards its citizens. Public service institutes offering citizens the opportunity to apply example of e-services.

- **E-society** initiatives : for business licenses through a government websites is one extend e-service domain by focusing on institutional stakeholders, such as private sector service providers, other public agencies, and not- for-profit and community organizations.E-society focuses on building long lasting partnerships and social/economical communities: for example through the creation of a business community portal

**Challenges of E-Governance :** one of the main challenges is**:**

**Governance networks**

Centre for Democratic Network Governance defines governance network as «  a horizontal articulation of independent, but operationally autonomous actors who interact through negotiations, transpiring within a regulative, normative, cognitive and imaginary framework that to acertain extent is self-regulating and which contribute to the production of public purpose within a particular area.

Governance network as a structure operates via horizontal relationships rather than a vertical, hierarchical chain of command of traditional bureaucratic structure of Max Weber.

Governance networks no longer use the traditional command-and-control relationship exemplified in bureaucratic systems. Network actors cooperate because they trust that the other actors will also play their part and fulfill their responsibilities.

***Legal terms***

|  |  |
| --- | --- |
| e- governance | الحوكمة الالكترونية  |
| Principles and objectives  | المبادئ والاهداف  |
| Accessibility  | النفاذ، الولوج، الوصول الى |
| Foster social inclusion  | تعزيز الادماج الاجتماعي  |
| Tax payers resources  | الموارد الضريبية  |
| Effectively and efficiently | بصفة فعالة وكفؤة |
| Transparency | شفافة |
| Efficiency | الكفاءة  |
| Objectivity | الموضوعية |
| Accountability | المسائلة  |
| Providing services | تقديم الخدمات |
| Cost effective services | خدمات فعالة من حيث التكلفة |
| Qualitative services | خدمات نوعية  |
| Government services | الخدمات الحكومية |
| A responsive administration | ادارة مستجيبة |
| Eliminate the middelmen | الغاء الوساطة |
| Civil society  | المجتمع المدني  |
| The internal working of the public sector | العمل الداخلي لللقطاع العام |
| Managing process performance | آداء إدارة وتسيير العمليات  |
| Empowerment | التمكين  |
| Business licences | التراخيص( الرخص) التجارية  |
| Institutional stackeholders | اصحاب الحصص ( المصالح) المؤسسين |
| Private sector  | القطاع الخاص |
| Service providers | مقدمي الخدمات  |
| Non-for- profit community oraganizations | مجموعة التنظيمات ( المنظمات) الغير ربحية  |
| Partnership | الشراكة  |
| Business community portal | بوابة مجتمع الاعمال  |
| Governance networks | شبكة الحوكمة  |
| Independent (autonomous) actors | الفواعل المستقلة  |
| Interact  | تفاعل  |
| Negociations | المفاوضات  |
| Regulative | تنظيمية |
| Normative | معيارية  |
| Cognitive | ادراكية( معرفية) |
| Framework  | إطار عمل  |
| Self regulating | تنظيم ذاتي  |
| Horizontal relationships | العلاقات الافقية  |
| Hierarchical chain of commands | سلسلة الاوامر السلمية (الهرمية= الرئاسية) |
| Bureaucratic structure | التنظيم الهيكلي البيروقراطي  |
| Cooperate | تتعاون  |

***الحوكمة الالكترونية ( الجزء 2)***

**مبادئ و أهداف الحوكمة المحلية:**

**مبادئ الحوكمة المحلية:**

-تقديم خدمات تأخذ بعين الاعتبار اختيارات المواطنين.

-زيادة النفاذ والوصول الى الحكومة

-تعزيز الادماج الاجتماعي

-نشر المعلومة بطريقة مسؤولة

-استعمال الموارد الضريبية بطريقة فعالة وكفؤة

**أهداف الحوكمة المحلية:**

-ضمان الشفافية في أعمال الحكومة .

-ضمان كفاءة، موضوعية، مساءلة أكثر، وسرعة في تقديم الخدمات والمعلومات للجمهور.

-تقديم خدمات نوعية وفعالة من حيث التكلفة.

-توفير شباك واحد لكل الخدمات الحكومية

-تطوير إدارة مستجيبة

-توفير واجهة مستخدم صديقة، سريعة وكفؤة.

-القضاء على الوساطة.

**مجالات الحوكمة الالكترونية:** هناك ثلاث مجالات رئيسية للحكومة الالكترونية وهي:

الادارة الالكترونية: وذلك بتحسين العمليات الحكومية

الخدمات الالكترونية : ربط المواطنين مع حكوماتهم.

المجتمع الالكتروني: بناء تفاعلات ضمن وبين المجتمع المدني.

**اولا: الادارة الالكترونية**: إن الهدف الرئيسي منهذه الاخيرة هو ترقية العمل الداخلي للقطاع العام باقتطاع تكاليف العمليات وآداء إدارة العمليات، وخلق تواصل استراتيجي بين هيئات الحكومة، والتمكين. كتقصير مدة الحصول على جوازات السفر من اسبوعين الى يوم واحد.

**ثانيا: الخدمات الاكترونية**

مبادرة تركز على تحسين العلاقة الحكومة ومواطنيها وذلك بزيادة تدفق المعلومات بينهم، وتنطوي على على اتصال ثنائي الاتجاه وتحسين مستوى الخدمات الحكومية اتجاه مواطنييها، حيث تمنح معاهد الخدمات العمومية للمواطنين فرصة وامكانية تطبيق نماذج عن الخدمات الالكترونية.

**ثالثا: المجتمع الالكتروني**

فالتراخيص التجارية، من خلال المواقع الحكومية تعد أحد مجالات الخدمة الالكترونية الممتدة بالتركيز على أصحاب الحصص( أصحاب المصالح) المؤسسين، مثل مقدمي الخدمات الخواص أو هيئات عمومية أخرى وليست مجموعة من المنظمات الغير ربحية.

كما يركز المجتمع الالكتروني على إقامة شراكة طويلة المدىومجموعات سوسيواقتصادية مثلا من خلال انشاء بوابة مجتمع الاعمال.

**تحديات الحوكمة الالكترونية**:

شبكة الحوكمة:

يعرفها مركز شبكة الحوكمة الديمقراطية بانها" تجمع افقي لفواعل مستقلة عمليا تتفاعل من خلال المفاوضات والترشح ضمن اطار عمل تنظيمي، معياري، ادراكي وافتراضي والى مدى معين تنظيم ذاتي والذي يسهم في انتاج أهداف معينة في مجالات معينة.

تعمل شبكة الحوكمة كهيكل من خلال العلاقات الافقية بدلا من العمودية ومن سلسلة اوامر هرميةللهيكل البيروقراطي التقليدي ل ماكس فيبر.

كما لا تستخدم علاقات الامر والرقابة التقليدية التي تجسد الانظمة البيروقراطية، حيث تتعاون فواعل الشبكة لثقتها بان باقي الفواعل ستلعب دورها وتقوم بمسؤولياتها.

**Master2/ Electronic Administration&Digital services**

***Text N° :06***

 ***The cybercrime***

 “Cybercrime” has been used to describe a wide range of offences, including offences against computer data and systems (such as “hacking”), computer-related forgery and fraud (such as “phishing”), content offences, and copyright offences (such as the dissemination of pirated content).

 It has evolved from the cyber-vandals to a range of profit-making criminal enterprises in a remarkably short time. Of course, criminals, like everyone else with accessand use of the Internet for communication and information gathering, and this has facilitated a number of traditional organized crime activities. But the growing importance of the Internet and our collective dependence on it has also created a number of new criminal opportunities. Asthe electronic hacking, transmitting contraband across borders through the Internet.

Cybercrime, or computer-oriented crime, is a crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime may threaten a person, company or a nation's security and financial health.There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state is sometimes referred to as cyberwarfare.

A report published in 2018, by [Center for Strategic and International Studies](https://en.wikipedia.org/wiki/Center_for_Strategic_and_International_Studies) (CSIS), concludes that close to $600 billion, nearly one percent of global gross product, is lost to cybercrime each year.

**Diffusion of cybercrime:**

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. Hacking has become less complex as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the  [computing](https://en.wikipedia.org/wiki/Cloud_computing) era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail [software-as-a-service](https://en.wikipedia.org/wiki/Software-as-a-service) is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for [spam](https://en.wikipedia.org/wiki/Email_spam).  computing could be helpful for a cybercriminal as a way to leverage his or her attack, in terms of brute-forcing a password, improving the reach of a [botnet](https://en.wikipedia.org/wiki/Botnet), or facilitating a spamming campaign.

***الجريمة السيبيرانية***

تم استخدام جرائم الانترنت للتعبير عن مجموعة واسعة من الجرائم، بما في ذلك الجرائم ضد بيانات وأنظمة الكمبيوتر كالقرصنة، التزوير والاحتيال المرتبط بالكمبوتر كالاختراق، ومخالفات المحتوى، وجرائم حقوق النشر( نشر محتوى تمت قصنته).

لقد تطورت هذه الجرائم من المخربين السيبيرانيين الى مجموعة من المؤسسات الاجرامية الربحية في وقت قصير بشكل جد ملحوظ، وبطبيعة الحال فإن المجرم مثل اي شخص آخر بامكانه النفاذ الى الانترنت واستخدامها للاتصال وجمع المعلومات مما سهل العديد من انشطة الجريمة المنظمة التقليدية. ولكن الاهمية المتزايدة للانترنت والاعتماد الجماعي عليها خلق العديد من الفرص والامكانيات الاجرامية الجديدة، مثل القؤصنة الالكترونية، نقل الممنوعات عبر الحدود من خلال الانترنت.

ان الجريمة السيبيرانية أو الجريمة الموجهة بالكومبيوتر هي جريمة تنطوي على حاسوب وشبكة، حيث يمكن استخدام الحاسوب في ارتكاب الجريمة، أو ان يكون هو الهدف

كما يمكن لهاته الجريمة أن تهدد أمن وسلامة الاشخاص أو الشركات أو الدول، لهذا نجد العديد من مخاوف الخصوصية تدور حول الجريمة الالكترونية، وذلك عندما يتم اعتراض المعلومات السرية أو الكشف عنها، قانونيا او بشكل آخر. وعلى الصعيد الدولي، فإن الفواعل الحكومية والغير حكومية تشارك في الجرائم الالكترونية بما في ذلك التجسس، الاختلاس، وغيرها من الجرائم العابرة للحدود. واحيانا يشار إلى الجرائم السيبيرانية العابرة للحدود والتي تنطوي على أعمال دولة قومية واحدة على الاقل باسم الحروب الالكترونية.

وقد خلص تقرير نشر عام 2018 من قبل مركز الدراسات الاستراتيجية الدولية إلى أن ما يقارب 600 بليون دولار، أي تقريبا 1% من اجمالي الناتج الاجمالي العالمي تتم خسارته بسبب الجرائم الالكترونية سنويا.

**انتشارالجرائم الإلكترونية:**

يعد الانتشار الواسع لأنشطة الجريمة الإلكترونية مشكلة في الكشف عن جرائم الكمبيوتر ومقاضاتها. حيث أصبحت القرصنة أقل تعقيدًا بحكم ماتقوم به جماعات القرصنة بنشر معارفها بشكل كبيرعبرالإنترنت.

 ساهمت المدونات والمجتمعات بشكل كبير في مشاركة المعلومات، إذ يمكن للمبتدئين الاستفادة من المعرفة التي يعرضها القراصنة المتمرسين ونصائحهم. علاوة على ذلك، فإن القرصنة متاحة بأرخص الاثمان أكثر من أي وقت مضى قبل عهد الحوسبة ، فمن أجل إرسال بريد عشوائيأ واحتيال، يحتاج المرء إلى خادم مخصص، ومهارات في إدارة الخادم، وإعدادات الشبكة، وصيانتها، ومعرفة معاييرالتزود بخدمة الإنترنت، وما إلى ذلك. مقارنة بذلك يعد برنامج البريد كخدمة إرسال قابلة للتطوير و غيرمكلفة ومجمعة وقابلة للتعامل لأغراض التسويق يمكن إعدادها بسهولة للبريد الإلكتروني العشوائي. حيث يمكن أن تكون الحوسبة مفيدة لمجرم الإنترنت كطريقة للاستفادة من هجومه، من حيث فرض كلمة مرور بطريقة آلية، أوتحسين وصول الروبوتات، أوتسهيل حملة البريد العشوائي.

**Master 2/electronic administration &digital services**

***Text N°: 07***

**Electronic contracts and consumer protection**

Vast technological advancement has made the lives of human beings more complex and this has inevitably extended to commercial transactions. The complexity of this problem has been accelerated by the growing popularity of standard form of contracts. In addition to the complexity of goods and services today, enormous changes have also occurred in the way consumers acquire these goods and services. In such a transaction, consumer has got no opportunity to suspect the genuineness of the person he/she is dealing with online and this places them at a greater risk of being swindled of their money by fraudsters. Consumers are often faced with unfair terms in the form of exemption clauses that attempt to exclude or limit the liability of trader. It is therefore essential that the government has authority, through appropriate legislations to protect its citizens through from unfair contract terms and other abusive market practices by manufacturers or retailers that are only interested in reaping large profits even at the expense of the unsuspecting consumers.

**Challenges posed by electronic contracts :** The advent of electronic commerce in modern commercial transactions has posed a great challenge on the law of sale of goods. E- Commerce allows consumers to purchase goods through transactions that are agreed, settled and transferred in an open network environment. As a result, there are several problems that are of concern to the consumers which needs to be addressed are:

1. **Privacy and data protection** Technology has played a great role in enhancing the capacity of internet companies to collect and analyze huge amounts of data relating to customers who merely visit their web sites, which raises concerns about how this data is treated. Many businesses around the world collect a variety of information on a regular basis about their own customer in order to understand their clients better, improve their business processes, and target special offers. customers to register with the company through websites by providing personal information. Another concern that consumers suffer from invading their own information is called “identity theft” when a thief gains access to personal information of a consumer which lets him impersonate the consumer and starts buying whatever goods and services which are to be billed to the consumer. Furthermore, usage of credit cards, debit cards, and smart cards can lead to recording, tracking and selling consumer’s shopping and banking practices.

2. **Product returns and refunds**: The other issue which arises in electronic contract is the right of the consumers to cancel the product after it is ordered by a party. Since the customer does not feel and touch the product, and consequently when the product arrives, the customer might not be satisfied with the product, the appearance of the product may not be as attractive as it seemed on the screen. This may defraud the consumers and as in a electronic contract the consumer is not provided with the right to inspect the goods.

 3. **Delivery of faulty goods**: The other issue in electronic contract related to the consumer when he receives faulty goods for totally wrong goods.

4. **Fixation of liability :** Another challenge with Electronic Contract is that it is very ambiguous to know as to who will owe the liability in case of some dispute arises in the manner as for delivery of dispute, late delivery etc. In electronic contract, however, the consumer discovers the misrepresentation only when he receives the goods or services. Further, it would be inconvenient for the consumer to return the goods and restore the benefits. In the same way the manufacturer or supplier of the goods and services can claim that they have entered into the contract with the online portal for the sale of the product or services and not have contrasted with the consumer. In United Kingdom, the Electronic Commerce( EC Directive) Regulation 2002 deal with this complex problem and it covers all the websitesselling goods and services online as ‘service providers’ and the liability is also imposed on these ‘service providers’ in case they does any act which goes against the interest of consumers and violates their consumer rights.

**Legal terms**

|  |  |
| --- | --- |
| Electronic contracts  | العقود الالكترونية  |
| consumer protection | حماية المستهلك  |
| Commercial transactions | المعاملات التجارية  |
| standard form of contracts | الشكل المعياري للعقود |
| Fraudsters | المحتالون |
| Unfair terms | الشروط الغير عادلة  |
| form of exemption clauses | شكل بنود الاعفاء |
| Exclude( limit) | تستبعد ( تحد) |
| The liability of traider  | مسؤولية التاجر |
| appropriate legislations | تشريعات مناسبة  |
| abusive market practices | ممارسات تجارية تعسفية  |
| Manifacturers | المصنعين  |
| Retailers | بائعي التجزئة  |
| the law of sale of goods | قانون بيع السلع  |
| Agreed  | اتفق |
| Settled ( settlment) | سوي ( تسوسة)  |
| Privacy and data protection | الخصوصية وحماية المعطيات  |
| Customers  | الزبائن، العملاء |
| Businesses | الشركات  |
| Regular bases | اسس قانونية ( نظامية) |
| business processes | العمليات التجارية  |
| Identity theft | سرقة الهوية  |
| access to personal information | النفاذ الى المعلومات الشخصية  |
| Banking practices | الممارسات البنكية  |
| Defraud the consumers  | الاحتيال على المستهلكين |
| the right to inspect the goods | حق تفتيش السلع |
| Fixation of liability  | تحديد المسؤولية  |
| Dispute | نزاع  |
| Faulty goods | السلع المعيبة  |
| Directive  | تعليمة  |
| Regulation  | تنظيم  |
| Interest of consumers  | مصلة المستهلك |
| To violate  | انتهك  |
| The consumer rights | حقوق المستهلك |

**العقود الالكترونية وحماية المستهلك :**

لقد جعلت التطورات التكنولوجية حياة الناس أكثر تعقيدا، وامتدت الى المعاملات التجارية، وقد تسارع هذا التعقيد من خلال الشيوع والانتشار الواسع للشكل المعياري للعقود، فبالإضافة إلى تعقيد السلع والخدمات، حدثت تحولات هامة في طريقة حصول المستهلكين على هذه السلع والخدمات، وفي مثل هذه المعاملات لا يكون للمستهلك اية امكانية للشك في صدق من يتعامل معهم عبر الانترنت وهو ما يجعله في خطر الوقوع بين ايدي المحتالين.

وعادة ما يواجه المستهلكون الشروط الغير عادلة للعقد في شكل بنود الإعفاء التي تسعى لاستبعاد مسؤولية التاجر أو الحد منها، لهذا بات من الضروري ان تحمي الحكومة بما لها من سلطة من خلال تشريعات مناسبة مواطنيها من الشروط الغير عادلة للعقد، ومن ممارسات السوق التعسفية الأخرى من قبل المصنعين وتجار التجزئة، الذين يسعون لجني الأرباح على حساب المستهلكين المطمئنين ( الواثقين).

**التحديات التي تفرضها العقود الالكترونية:**

لقد فرض دخول التجارة الالكترونية الى المعاملات التجارية المعاصرة تحديات كبيرة على قانون بيع السلع ، حيث تسمح التجارة الالكترونية للمستهلكين باقتناء السلع عبر المعاملات التي اتفقوا عليها وسووها وحولوها عبر بيئة الشبكات، ويترتب عن هذا العديد من المسائل في غاية الأهمية بالنسبة للمستهلك والتي يجب معالجتها:

1-**الخصوصية وحماية المعلومات**: لقد لعبت التكنولوجيا دورا كبيرا في تعزيز قدرة شركات الانترنت لجميع وتحليل البيانات المتعلقة بالمستهلكين الذين يزورون مواقعها، وهو الأمر الذي يثير التشاؤل حول كيفية معالجة هذه البيانات، فالعديد من الشركات حول العالم تجمع المعلومات على أسس قانونية حول زبائنها حتى تتفهمهم أكثر، وتحسين عملياتهم التجارية، واستهداف العروض الخاصة، حيث يسجل العملاء بياناتهم الخاصة عبر مواقع الشركات، كما يعاني المستهلكون من اختراق معلوماتهم الشخصية من خلال مايعرف بسرقة الهوية، عندما يلج اللص الى المعلومات الشخصية للمستهلك وانتحال شخصيته والقيام بشراء السلع والتزود بالخدمات بموجب فواتير باسم المستهلك، اضف الى ذلك استعمال بطاقات الائتمان والاقتراض والبطاقات الذكية مما يؤدي الى تسجيل وتتبع ممارسات والخدمات المصرفية للمستهلكين وبيعها.

2**-ارجاع المنتج والمبالغ المستردة:** من بين المسائل الهامة في العقود الالكترونية، حق المستهلك في الغاء المنتجات بعد طلبها من أحد الأطراف، فمادام االزبون لم يرى ولم يلمس المنتج، ولما يصل اليه هذا الاخير، قد لا يرضيه، فمظهر المنتج في الحقيقة يختلف عنه في الشاشة، وهو ما يجعل المستهلك عرضة للاحتيال خاصة و أنه يفتقد الى الحق في تفتيش المنتج والتحقق منه.

**3-تسليم المبيع المعيب**: وهي مسألة أخرى تهم المستهلك عند استلامه للمبيع المعيب المخالف تماما للسلع المطلوبة.

4**- تحديد المسؤولية**: وهو تحد آخر للعقود الالكترونية، فليس من الواضح معرفة من يتحمل المسؤولية في حالة النزاعات التي تتعلق بالتسليم وبالتأخر في التسليم.

 ففي العقود الالكترونية، يكتشف المستهلك التحريف فقط عند تلقي السلع والخدمات، بل أكثر من ذلك يكون من غير الملائم بالنسبة للمستهلك ارجاع السلع واسترداد المبالغ، كما أن المصنع او التاجر يمكنه الدفع بأنه تعاقد مع المستهلك عبر بوابة الكترونية لبيع المنتج او الخدمات، ولم يكن هناك اعتراض من المستهلك.

ففي المملكة المتحدة حسب التعليمة ( التنظيم 20002) الذي يتعامل مع هذه المسالة المعقدة، حيث تغطي التجارة الالكترونية كل مواقع البيع السلع والخدمات عبر الخط، كمزودي خدمات وهنا تقوم مسؤوليتهم في حالة ارتكابهم لاي تصرفات تتعارض مع مصلحة المستهلك وتنتهك حقوقه.

**Master 2/electronic administration &digital services**

***Text N°: 08***

**Information Security in The Algerian Law**

Information security means: to provide protection for information from the risks that threaten it, or the barrier that prevents its misuse, by providing tools, means, standards and measures taken to prevent information from reaching the hands of unauthorized persons through communications, and to ensure its authenticity and validity.

**1/Information Security in the Penal Code** : The Algerian legislator rectified the legal vacuum in the field of combating cybercrime achieving information security, especially cyber crimes under Law 15-04 containing the amendment of the Penal Code, according to which some acts related to automatic data processing are criminalized, and these actions are as follows:

1. **The crime of unauthorized entry**: This crime is based on unauthorized access to the information system; It has been indicated by article 394 bis of the Algerian Penal Code, where the penalty is: imprisonment from 3 months to a year, and a fine from 50,000 to 100,000 DZA, Anyone who fraudulently enters or remains in all or part of the automated data processing system or tries to do so, and the penalty is doubled if that results in the deletion or change the system’s data or sabotage the system’s works system.
2. **The crime of information fraud**: Involves "manipulating" the data contained in the data processing system,2 It is limited to acts of insertion, deletion, and modification, by entering new incorrect data or amending the last existing one list; where the legislator decided for her the penalty of imprisonment and a fine with the possibility of doubling the penalty.

3- **The crime of data seizure**: This crime is the most prevalent in the hypothetical world, as it involves designing, researching, gathering, providing, publishing, or trading in data stored, sent or processed by an information system, Or the possession, creation, publication, or use of data obtained from one of the crimes stipulated in Section Four of the Algerian Penal Code, for any purpose whatsoever. And the perpetrator is punished with imprisonment from two months to 03 years and a fine of 1,000,000 to 5,000,000 DZD.

**4/The Crime of vandalism and destruction of Data**: The Algerian legislator defined it as: "Whoever enters by Cheat Data in the automatic processing system or Cheat removing or modifying the data contained in Section 05 of the Penal Code". It has approved the penalty of imprisonment and a fine for those who commit it.

 5- **Information fraud crime**: in the Penal Code in Article 394 bis 02: "Everyone who cheats, Designing, researching, collecting, presenting, publishing, or commodity data stored, processed, or transmitted through the information system. and Acknowledged the penalty of imprisonment and a fine for the perpetrators."

6- **Crimes related to Internet activities**: Stipulated in the articles of Section Four bis of the Algerian Penal Code, especially Article 394 bis 2/2: "Acts of possession, disclosure and publication that occur on automatic data, with the aim of unfair competition, espionage, terrorism, incitement to immorality, and all unlawful acts". (This is a broad term that could include any business within the scope of this type of cybercrime). The penalty for this is: Imprisonment and a fine in addition to a complementary penalty, which is: Closing down sites are the subject of these crimes. And the confiscation of the devices, programs and means used, with an increased penalty if the crime targets national defense or the bodies and institutions subject to public law.

Moreover ; The Algerian legislature has decided to protect people from infringing on the sanctity of their private lives, by capturing, recording or transmitting private or secret calls or conversations, or pictures in a private place without the permission or consent of the owner.

**Legal terms** :

|  |  |
| --- | --- |
| Information security  | الامن السيبيراني  |
| The algerian law | القانون الجزائري  |
| Risks  | المخاطر  |
| To threaten ( a threat)  | يهدد ( التهديد) |
| Prevent (prevention) | الوقاية ( المنع) |
| An Unathorized person | شخص غير مرخص به |
| Authenticity | الاصالة |
| Validity | الصلاحية  |
| The algerian legislator | المشرع الجزائري |
| The legal vaccum | الفراغ القانوني  |
| Combating cybercrime | محاربة الجريمة السيبيرانية  |
| The amendment of the penal code | تعديل قانون العقوبات  |
| Automatic data processing | المعالجة الالية للمعلومات  |
| Criminalized | مجرم (مجرمة) |
| The crime of unauthorized entry | جريمة الدخول الغير مرخص به |
| An unauthorized acess  | النفاذ الغير مرخص به |
| The penalty of Imprisonment | عقوبة الحبس |
| A fine | غرامة |
| The crime of information fraud | جريمة تزوير المعلومات |
| The crime of data seizure | جريمة حجز البيانات |
| The possession | الحيازة  |
| Stipulated | المنصوص عليه |
| The perpetrator is punished | يعاقب الفاعل( المجرم= مرتكب الجريمة)  |
| The crime of vandalism and destruction of data | جريمة تخريب البيانات واتلافها  |
| By cheat( to cheat) | عن طريق الغش( يغش) |
| Information fraud crime | جريمة الاحتيال المعلوماتي |
| Article 120 bis  | المادة 120 مكرر  |
| Disclosure | الافصاح  |
| Unfair competition | المنافسة الغير مشروعة  |
| Espionage | التجسس |
| Terrorism | الارهاب |
| Unlawfull acts | التصرفات الغير قانونية( الغير شرعية) |
| Complementary penalty | عقوبة تكميلية |
| Confiscation | مصادرة |
| Increased penalty | عقوبة مشددة  |
| National defense | الدفاع الوطني  |
| Bodies and institutions subject to public law | الهيئات والمؤسسات الخاضعة للقانون العام |
| Infringing on the sanctity of the private live | اعتداء على حرمة الحياة الخاصة |
| Permission or consent of the owner | اذن او رضا صاحبها |

***الأمن المعلوماتي (السيبيراني) في القانون الجزائري***

يعني الامن المعلوماتي توفير الحماية للمعلومات من المخاطر التي تهددها او الحواجز التي تمنع من سوء استعمالها وذلك بتوفير الوسائل والادوات و المعايير والاجراءات المتخذة لحماية المعلومة من الوصول الى ايدي الاشخاص الغير مرخص لهم، ولضمان اصالتها وصلاحيتها.

الامن المعلوماتي في قانون العقوبات: لقد تدارك المشرع الجزائري الفراغ القانوني في مجال محاربة الجريمة السيبيرانية التي تمس بامن المعلومات، خاصة الجرائم الالكترونية بموجب القانون 04/15المتضن تعديل قانون العقوبات، والذي تكون حسبه بعض التصرفات المتعلقة بالمعالجة الالية للبيانات مجرمة، والتي تتمثل فيما يلي:

1-جريمة الدخول الغير مرخص به: وهي قائمة اساسا على النفاذ الغير مرخص به لنظام المعلومات، وقد اشير اليها بموجب نص المادة 394 مكرر من قانون العقوبات الجزائري حيث تكون العقوبة من ثلاثة اشهر حبس الى سنة وغرامة من 50 الف الى 100 الف دج، فكل من يدخل عن طريق الغش او يبقى في كل أو في جزء من منظومة المعالجة الالية للبيانات او يحاول ذلك ، كما تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات النظام أو تخريب لمنظومة اشتغال النظام.

2-جريمة تزوير المعلومات: وتشمل التلاعب بالبيانات المتضمنة في نظام المعالجة الالية، وتقتصر على تصرفات

( اعمال) الادراج، الحذف والتعديل وذلك بادخال بياناتات جديدة غير صحيحة او تعديل الموجودة سابقا، حيث قرر لها المشرع عقوبة الحبس وغرامة مع امكانية مضاعفة العقوبة.

3-جريمة حجز البيانات: وهي السائدة اكثر في العالم الافتراضي، حيث تشمل تصميم، البحث، الجمع، تقديم ونشر أو الاتجار بالبيانات المخزنة، المرسلة أو المعالجة في نظام المعلومات، أو حيازة، إفشاء او استعمال البيانات المتصل عليها من احدى الجرائم المنصوص عليها في القسم الرابع من قانون العقوبات لأي غرض مهما كان.

ويعاقب الفاعل بالحبس من شهرين الى ثلاثة سنوات وغرامة من مليون الى 5 ملايين دج.

4-جريمة تخريب المعطيات واتلافها: يعرفها المشرع الحزائري بانها( كل من ادخل عن طريق الغش بيانات في نظام المعالجة الالية للمعطيات أو أزال أو عدل عن طريق الغش المعطيات المحتواة في الفرع الخامس من قانون العقوبات، واقر عقوبة الحبس والغرامة لمرتكبها.

5-جرائم الاحتيال المعلوماتي: جاء في المادة 394 مكرر 2 كل من يقوم عن طريق الغش بالتصميم، البحث، الجمع، توفير، نشر او الاتجار بالبيانات المخزنة، المعالجة أو المحولة من خلال نظام المعلومات ، ويقرر عقوبة الحبس والغرامة على مرتكبيها.

6-الجرائم المتعلقة بنشاطات الانترنت والتي نص عليها في مواد القسم الرابع مكرر من قانون العقوبات، خاصة المادة 394مكرر 2/2 " اعمال الحيازة والنشر التي تقع على البيانات الالكترونية بهدف المنافسة الغير مشروعة، التجسس، الارهاب، التحريض على الفسوق، وكل التصرفات الغير شرعية"( وهو المعنى الاوسع الذي يمكن ان يشمله أي عمل ضمن نطاق هذا النوع من الجرائم الالكترونية).

والعقوبة هي الحبس والغرامة إضافة إلى العقوبة التكميلية المتمثلة في غلق المواقع محل الجريمة. ومصادرة الأجهزة، البرامج، والوسائل المستعملة، مع تشديد العقوبة اذا استهدفت الجريمة الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام.

اكثر من ذلك، فقد قرر التشريع الجزائري حماية الاشخاص من التعدي على حرمة حياتهم الخاصة من خلال رصد والتقاط، تسجيل ونقل الاتصالات والمحادثات السرية والخاصة ، أو الصور في أماكن خاصة دون إذن ورضا صاحبها.

**Master 2/electronic administration &digital services**

***Text N°: 09***

**Information Security in The Algerian Law ( part 2)**

B**) Information Security in the Criminal Procedures Law:**

The Algerian legislator, through Article 37 of the Code of Criminal Procedure, has given local jurisdiction to the Procurator of the Republic in information crimes, stipulated the inspection in Article 45, paragraph 07 thereof. And on arrest for consideration of In the crime infringing processing systems in the text of Article 51, paragraph 06 thereof, and

the interception of correspondence, recording of votes and taking pictures in Article 65 bis 05 to 65 bis 10, as for the investigation and trial procedures, the same procedures of the traditional crime shall be applied to it.

**C -information security in private laws**: Due to the extension of the threat of cybercrime in all areas of life, it was necessary to stipulate it even in special laws, including:

1- **Industrial property laws**: The legislator has touched on the regulation of trademark provisions in Ordinance No. 03-06 related to trademarks, by registering the program under a trademark name for it, but the matter is related to the protection of the name only without the content and it is a protection that may be effective by simple and not complex copying. As for computer information programs, the Algerian legislator explicitly excluded them from the field of patent protection.

2**- Literary property laws**: With the remarkable development in the field of communication in recent times, the means of transporting intellectual production in various forms have developed with it. The Algerian legislature has expanded, through Order 97-10 amended and supplemented by Order 03-05 of the list of protected literature, as it incorporated media applications within the original works that were expressed in database works and computer programs that enable managed to do activity scientific, or any activity to obtain On a special result of the information, that read with a machine. Penalties are also increased for those who violate the rights of authors, especially authors of Informatics works.

D) **Information Security in the Law on Combating Media and Communication Technology Crimes**:Law No. 09-04 was promulgated in Algeria, Includes rules for prevention and control of crimes related to information and communication technology, whereby it is permissible to monitor electronic information in terrorism-related matters in violation of public order. This law aims to protect the automatic data processing systems from crimes, and it also has a scope for investigation. Given the confidentiality of communications, the seriousness of potential threats, and the importance of the protected interests, the requirements of theprotection of the public order or its requirements can monitor electronic communications, collect and record their content, and carry out inspection or seizure Within information systems.

Electronic communications can also be monitored to prevent acts described as crimes of terrorism, sabotage, and crimes that affect the security of the state, or provide information about a possible attack on an information system in a manner that threatens state institutions or national defense. And for the public Prosecutor at the Algerian Judicial Council is authorized to grant judicial police officers a minimum period of 6 months, which can be extended. This law stipulated in its third chapter the procedural rules own for the inspection process in the field of crimes related to information and communication technologies in accordance with applicable global standards, with the possibility of resorting to the assistance of the competent foreign authorities in order to inspect the information systems located abroad. As well as withholding data and data, preventing access to data on the content of the offense, and saving traffic data according to Article 10 of Law 09-04. In addition to the obligations of Internet service providers to prevent access to data contrary to public order, which constitute a crime, by pulling their contents, and to establish technical arrangements to prevent access to it according to Article 12 of Law 09-04. Chapter five of this law also stipulates the establishment of a national commission for the prevention and control of crimes related to information and communication technology, which will coordinate and activate the prevention of media crimes and assist the judicial authorities and judicial police services in their investigations regarding crimes, on media-related crimes according to Article 14 of the same law. And the Algerian courts have jurisdiction if the crimes are committed outside the Algerian territory, when the perpetrators are foreigners, and are targeting state institutions, and international judicial assistance may be requested on the condition that sovereignty is not violated.

**Legal terms**

|  |  |
| --- | --- |
| Information Security in the Criminal Procedures Law: | الامن المعلوماتي في قانون الاجراءات الجزائية |
| The algerian legislator | المشرع الجزائري |
| the Code of Criminal Procedure | قانون الاجراءات الجزائية |
| local jurisdiction  | الاختصاص القضائي المحلي  |
| the Procurator of the Republic | وكيل الجمهورية |
| information crimes | جرائم المعلوماتية |
| stipulated the inspection  | نصت على التفتيش |
| arrest for consideration | التوقيف للنظر  |
| Crime infringing processing systems | جرائم الاعتداء على أنظمة المعالجة |
| Investigation | التحريات ( التحقيقات) |
| Trial procedures | اجراءات المحاكمة |
| Private laws | القوانين الخاصة |
| Industrial property laws | قوانين الملكية الصناعية |
| Regulation of the trademark provisions  | تنظيم احكام العلامة التجارية |
| Ordinance | الامر |
| Pattern protection | حماية براءة الاختراع |
| Literary property laws | قوانين الملكية الادبية( الفكرية) |
| The Order amended and supplemented | الامر المعدل والمتمم |
| To violate  | ينتهك |
| The rights of authors | حقوق المؤلف |
| Law of combating media and C T crimes  | قانون مكافحة جرائم الاعلام وتكنولوجيا الاتصال |
| Promulgated | الصادر |
| Rules for prevention and control of crimes | قواعد للوقاية ورقابة الجرائم  |
| To monitor electronic information | رقابة المعلومات الالكترونية  |
| Violation of public order | المخالفة للنظام العام  |
| Scope of investigation | نطاق التحري |
| Confidentiality  | سرية |
| Potential threats | التهديدات المحتملة |
| To carry out  | ينفذ |
| Inspection or seizure | التفتيش او الحجز |
| Crimes of sabotage and terrorism | جرائم التخريب والارهاب |
| Security of state | امن الدولة |
| State institutions | مؤسسات الدولة |
| Public prosecutor | المدعي العام  |
| The judicial council | المجلس القضائي |
| Authorized | ياذن  |
| Judicial police officers | ضباط الشرطة القضائية |
| Procedural rules | القواعد الاجرائية |
| Applicable global standards | المعايير العالمية المطبقة |
| The competent foreign authorities | السلطات الاجنبية المختصة |
| Obligations | التزامات |
| Contrary to public order | المخالفة للنظام العام |
| To establish arrangments | وضع ترتيبات  |
| Media crimes | جرائم الاعلام |
| Judicial authorities | السلطات القضائية |
| Judicial police services | مصالح الشرطة القضائية |
| International judicial assistance | المساعدة القضائية الدولية  |
| The sovereignity  | السيادة  |
| Not violated | لا تنتهك  |

**الامن المعلوماتي في القانون الجزائري ( الجزء الثاني).**

**الامن المعلوماتي في قانون الاجراءات الجزائية:**

لقد منح المشرع الجزائري بموجب المادة 37 من قانون الاجراءات الجزائية الاختصاص القضائي لوكيل الجمهورية في جرائم المعلوماتية بالنص على التفتيش في المادة 45/7 منه، والتوقيف للنظر في جرائم الاعتداء على انظمة المعالجة بموجب المادة 51/6 وكذا اعتراض المراسلات، تسجيل الاصوات، والتقاط الصور بموجب المادة 65 مكرر/5 ، و المادة 65 مكرر 10، اما بالنسبة للتحريات واجراءات المحاكمة فهي نفسها المقررة والمطبقة في الجرائم التقليدية

جرائم الامن المعلوماتي في القوانين الخاصة: بالنظر الى تهديدات الجرائم الالكترونية التي امتدت الى كل مجالات الحياة، كان من الضروري النص عليها في قوانين خاصة منها:

1. **قوانين الملكية الصناعية:** حيث جسد المشرع ذلك بتنظيم احكام العلامات التجارية في الامر 03/06 المتعلقة بالعلامة التجارية، من خلال تسجيل برامج تحت اسم العلامة التجارية، ولكن المسالة المتعلقة بالحماية فقد مست الاسم فقط دون المحتوى وهي حماية يمكن أن تكون فعالة من خلال نسخ بسيط وغير معقد. وبالنسبة لبرامج معلومات الكمبيوتر فقد استبعدها المشرع الجزائري صراحة من مجال حماية براءة الاختراع .
2. **قوانين الملكية الأدبية**: مع التطورات الملحوظة في مجال المعلوماتية، والتي مست مختلف وسائل نقل الانتاج الفكري، حيث وسع المشرع الجزائري من خلال الامر 97/10 المعدل والمتمم بالامر 03/05 من قائمة المنتجات المحمية، حيث دمج تطبيقات الوسائط ضمن المصنفات الاصلية المعبر عنهافي اعمال قاعدة البيانات وبرامج الكمبيوتر التي تمكن من القيام بالنشاطات العلمية أو أي نشاط للحصول على نتائج خاصة بالمعلومة التي تقرا آليا. حيث تشدد العقوبات على من ينتهك حقوق المؤلف وخاصة المؤلفين في مجال الاعمال المعلوماتية.
3. **الأمن المعلوماتي في قانون مكافحة جرائم الإعلام وتكنولوجيا الاتصال** : يضم القانون 09/04 الصادر في الجزائر قواعد للوقاية والرقابة على الجرائم المتعلقة بالمعلومات وتكنولوجيا الاتصال والذي يجيز بموجبه بمراقبة المعلومات الالكترونية في الامور المتعلقة بالارهاب والمخالفة للنظام العام.

حيث يهدف هذا القانون لحماية انظمة المعالجة الالية للبيانات من الجرائم وتحديد نطاق التحريات، وبالرغم من سرية الاتصالات وجدية التهديدات المحتملة، و أهمية المصالح المحمية، فإن متطلبات حماية النظام العام يمكن ان تراقب المعلومات الالكترونية لجمع وتسجيل محتواها وتنفيذ التفتيش والحجز داخل نظام المعلومات.

كما يمكن مراقبة الاتصالات الالكترونية للوقاية من التصرفات التي يمكن وصفها بجرائم الارهاب، التخريب، والجرائم التي تمس امن الدولة أو تقدم المعلومة حول الاعتداءات الممكنة على نظام المعلومات بطريقة تهدد مؤسسات الدولة والدفاع الوطني، وبالنسبة للنائب العام لدى مجلس قضاء الجزائر فانه يمنح الاذن لضباط الشرطة القضائية لمدة ستة اشهر قابلة للتمديد.

حيث نص هذا القانون في الفصل الثالث منه على القواعد الاجرائية الخاصة بعملية التفتيش في مجال الجرائم المتعلقة بالمعلومات وتكنولوجيا الاتصال وفقا للمعايير العالمية المطبقة، مع امكانية اللجوء الى مساعدة السلطات الاجنبية المختصة بهدف تفتيش( مراقبة ) انظمة المعلومات الموجودة في الخارج.

إضافة الى حجب البيانات، منع النفاذ الى البيانات المتعلقة بمحتوى الجريمة وحفظ بيانات حركة السير وفقا للمادة 10 من القانون 09/04. بالاضافة الى التزامات مقدمي خدمات الانترنت لمنع الوصول الى البيانات المخالفة للنظام العام والتي تشكل جريمة من خلال سحب محتوياتها ووضع تدابير ( ترتيبات تقنية) لمنع الوصول اليها حسب المادة 12 من القانون 09/04.

كما نص الفصل الخامس على انشاء لجنة وطنية للوقاية من الجرائم المتعلقة بالمعلومات وتكنولوجيا الاعلام ومكافحتها والتي تتولى التنسيق والتفعيل من أجل منع الجرائم الالكترونية وتساعد السلطات القضائية ومصالح الشرطة القضائية في تحقيقاتهم اتجاه الجرائم المتعلقة بالاعلام حسب نص المادة 14 من نفس القانون، كما ان للمحاكم الجزائرية الاختصاص القضائي إذا ما تم ارتكاب هذه الجرائم خارج الاقليم الجزائري عندما يكون الفاعلون اجانب ويستهدفون مؤسسات الدولة، وهنا تكون المساعدة القضائية مطلوبة بشرط ان لاتنتهك السيادة.