Faculty of law and political sciences
Department of law
Master 2/ Criminal law
Texts of English module

الفئة المستهدفة: طلبة السنة الثانية ماستر تخصص القانون الجنائي

من اعداد الاستاذة: زراري حبيبة

السنة الجامعية: 2023/ 2024

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 access and 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. As the 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 (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 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 is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for 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, or facilitating a spamming campaign.

Legal terms

Cybercrimes	الجريمة الالكترونية (السيبيرانية)
Offences	الاعتداءات(الجرائم)
hacking	القرصنة
computer-related forgery and fraud	التزوير والاحتباط المرتبط بالكمبيوتر
Content offences	جرائم المحتوى
Copyright offences	جرائم حقوق النشر
the dissemination of pirated content).	نشر المحتوى المقرصن
Cyber vadals (vandalism)	المخربين (التخريب) الالكترونيين
Criminal enterprises	مؤسسات اجرامية
Criminals	مجرمين
Criminal opportunities	الفرص الاجرامية
Threaten	تهدد
Nation security	أمن الدولة
Company	المؤسسات
Commission of a crime	ارتكاب الجريمة
Interception and disclosure	اعتراض وافصاح
Lawfully	بطريقة قانونية
Governmental actors	فواعل حكومية
Non-state actors	فواعل غير دولاتية (غير حكومية)
Engage	تشترك
Espionage	التجسس

الجرائم العابرة للحدود	Croos-border crimes
الحرب الالكترونية	Cyberwarefare
الكشف والتحقيق بشأن الجرائم الالكترونية	Computer crimes detection and prosecution

الجريمة السيبيرانية

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

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 القرصنة 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.

انتشار الجرائم الإلكترونية:

يعد الانتشار الواسع لأنشطة الجريمة الإلكترونية مشكلة في الكشف عن جرائم الكمبيوتر ومقاضاتها. حيث أصبحت القرصنة أقل تعقيدًا بحكم ما تقوم به جماعات القرصنة بنشر معارفها بشكل كبيرعبرالإنترنت،وقد 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 وغيرمكلفة 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/ Criminal law

Text N°:02

The International Criminal Court

The **International Criminal Court** (**ICC** or **ICCt**) is an international tribunal that sits in The Hague, Netherlands. The ICC is the first and only permanent international court with jurisdiction to prosecute individuals for the international crimes of genocide, crimes against humanity, war crimes and the crime of aggression. It is intended to complement existing national judicial systems, and it may, therefore, exercise its jurisdiction only when national courts are unwilling or unable to prosecute criminals. The ICC lacks universal territorial jurisdiction and may only investigate and prosecute crimes committed within member states, crimes committed by nationals of member states, or crimes in situations referred to the Court by the United Nations Security Council.

The ICC began operations on 1 July 2002, upon the entry into force of the Rome Statute, a multilateral treaty that serves as the court's foundational and governing document. States which become party to the Rome Statute become members of the ICC, serving on the Assembly of States Parties, which administers the court. As of December 2020, there are 123 ICC member states; 42 states have neither signed nor become parties to the Rome Statute.

The ICC has four principal organs: the Presidency, the Judicial Divisions, the Office of the Prosecutor and the Registry. The President is the most senior judge chosen by his or her peers in the Judicial Division, which hears cases before the Court. The Office of the Prosecutor is headed by the Prosecutor who investigates crimes and initiates criminal proceedings before the Judicial Division. The Registry is headed by the Registrar and is charged with managing all the administrative functions of the ICC, including the headquarters, detention unit, and public defense office.

Following the Second World War, the allied powers established two *ad hoc* tribunals to prosecute Axis leaders accused of war crimes. The International Military Tribunal, which sat in Nuremberg, prosecuted German leaders while the International Military Tribunal for the Far East in Tokyo prosecuted Japanese leaders. In 1948 the United Nations General Assembly first recognised the need for a permanent international court to deal with atrocities of the kind prosecuted after the Second World War. At the request of the General Assembly, the International Law Commission (ILC) drafted two statutes by the early 1950s but these were shelved during the Cold War, which made the establishment of an international criminal court politically unrealistic.

Legal terms :

The international criminal court	المحكمة الجنائية الدولية

International tribunal	المحكمة الدولية
permanent international court	محكمة دولية دائمة
jurisdiction	اختصاص قضائي(ولاية قضائية)
to prosecute individuals	متابعة الافراد
the international crimes	الجرائم الدولية
Genocide	جريمة الإبادة
Crimes against humanity	الجرائم ضد الإنسانية
War crimes	جرائم الحرب
The crime of agression	جريمة العدوان
national judicial systems	الأنظمة القضائية الوطنية
national courts	المحاكم الوطنية
Criminals	المجرمون
universal territorial jurisdiction	الاختصاص القضائي الاقليمي العالمي
To investigate (investigation)	التحقيق
Member states	الدول الاطراف
United Nations Security Council	مجلس الامن الاممي
the entry into force of the Rome Statute	دخول النظام الاساسي لروما حيز النفاذ
Multilateral treaty	معاهدة متعددة الاطراف
court's foundational and Governing document	الوثيقة التاسيسة والناظمة للمحكمة
the Presidency	الرئاسة
the Judicial Divisions	الشعب القضائية
the Office of the Prosecutor	مكتب المدعي
the Registry	قلم الحكمة
Criminal proceedings	الاجراءات الجزائية
detention unit	وحدة الاحتجاز
public defense office	مكتب الدفاع العام
Had hoc tribunals	محاكم خاصة
Accused	متهم
The International Military Tribunal	المحكمة العسكرية الدولية

United Nations General_Assembly	الجمعية العامة للامم المتحدة
the International Law Commission	لجنة القانون الدولي
To draft	صاغ (صياغة)

المحكمة الجنائية الدولية

إن المحكمة الجنائية الدولية هي محكمة دولية، مقرها لاهاي، هولندا، وكانت أول محكمة جنائية دائمة التي لها اختصاص متابعة الأفراد عن الجرائم الدولية كالإبادة الجماعية، الجرائم ضد الإنسانية، جرائم الحرب وجريمة العدوان، ويمتد عملها لإكمال الأنظمة القضائية الوطنية الموجودة، حيث تمارس اختصاصها عندما لا ترغب أو لاستطيع الدول متابعة المجرمين، و تفتقر المحكمة الجنائية الدولية إلى الولاية القضائية الإقليمية العالمية ويمكنها فقط التحقيق والملاحقة القضائية في الجرائم المرتكبة داخل الدول الأعضاء، أو الجرائم التي يرتكبها مواطنو الدول الأعضاء، أو الجرائم في الحالات المحالة إلى المحكمة من قبل مجلس الأمن التابع للأمم المتحدة.

وقد بدات عملها في اول جويلية 2002، اي مع دخول نظام روما الأساسي حيز التنفيذ، وهي معاهدة متعددة الأطراف تعمل بمثابة الوثيقة التأسيسية والناظمة للمحكمة. فالدول الأطراف في نظام روما الأساسي أصبحت أعضاء في المحكمة الجنائية الدولية، وتعمل في جمعية الدول الأطراف، التي تدير المحكمة. اعتبارًا من ديسمبر 2020، كان هناك 123 دولة عضو في المحكمة الجنائية الدولية؛ 42 منها لم توقع ولم تصبح أطرافا في نظام روما الأساسي.

تضم المحكمة الجنائية الدولية أربعة أجهزة رئيسية: الرئاسة، الشعب القضائية، ومكتب المدعي العام وقلم المحكمة. الرئيس هو أقدم قاضٍ يتم اختياره من قبل أقرانه في الدائرة القضائية التي تنظر في القضايا المعروضة على المحكمة. يرأس مكتب المدعي العام المدعي العام الذي يحقق في الجرائم ويباشر الإجراءات الجنائية أمام الدائرة القضائية.

يرأس قلم المحكمة مسجل وهو مكلف بإدارة جميع الوظائف الإدارية للمحكمة الجنائية الدولية، بما في ذلك المقر، ووحدة الاحتجاز، ومكتب الدفاع العام.

بعد الحرب العالمية الثانية، أنشأت القوى المتحالفة محكمتين خاصتين لمحاكمة قادة المحور المتهمين بارتكاب جرائم حرب. حيث حاكمت المحكمة العسكرية الدولية التي انعقدت في نورمبرج قادة ألمان، بينما حاكمت المحكمة العسكرية الدولية للشرق الأقصى في طوكيو قادة يابانيين.

وفي عام 1948، أقرت الجمعية العامة للأمم المتحدة لأول مرة بالحاجة إلى محكمة دولية دائمة للتعامل مع الفظائع من النوع الذي تمت مقاضاته بعد الحرب العالمية الثانية. وبناءًا على طلب من الجمعية العامة، صاغت لجنة القانون الدولي (ILC) نظامين أساسيين بحلول أوائل الخمسينيات من القرن الماضي، لكن تم وضعهما على الرف أثناء الحرب الباردة، مما جعل إنشاء محكمة جنائية دولية أمرًا غير واقعي من الناحية السياسية.

Master 2/ criminal law

Text N°: 03

Juvenile justice

Juvenile justice As stated through out the Guidance, juvenile justice (or children's justice, as it is sometimes referred to) is a general term used to describe the policies, strategies, laws, procedures and practices applied to children over the minimum age of criminal responsibility who have come into conflict with the law. the term 'juvenile justice' needs to be distinguished from the broader concept of 'justice for children', which covers children in conflict with the law (i.e. alleged as, accused of, or recognised as having infringed the penal law), children who are victims or witnesses of crime, and children who may be in contact with the justice system for other reasons such as custody, protection or inheritance. Albeit there is no generally accepted definition of the term 'juvenile', it is often used to signify a child who is over the minimum age of criminal responsibility and is alleged to, accused of, or convicted of a criminal offence. The United Nations Rules for the Protection of Juveniles Deprived of their Liberty (the 'Havana Rules') simply define a juvenile as 'every person under the age of 18.' The United Nations Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules) provide the following definition: 'A juvenile is a child or young person who under the respective legal system may be dealt with for an offence in a manner which is different from an adult'. The Committee on the Rights of the Child (CRC) avoids the use of the term juvenile, referring instead to "children in conflict with the law.

The 1985 Beijing Rules and The Riyadh Guidelines established basic actions to prevent children and young people from engaging in criminal activities, as well as to protect the human rights of youth already found to have broken the law. In 1989, the focus on safeguarding the human rights of children and young people was strengthened by the

Convention on the Rights of the Child (CRC), which entered into force in 1990. In 1995, the United Nations adopted the World Programme of Action for Youth (WPAY), providing a policy framework and practical guidelines for national action and international support to improve the situation of young people.

Through the WPAY, the United Nations puts forth policy actions specifically tailored to young people between 15 and 24 years of age. The World Programme of Action for Youth aims at fostering conditions and mechanisms to promote improved well-being and livelihoods among young people. As such, it requires that Governments take effective action against violations of all human rights and fundamental freedoms and promote non-discrimination, tolerance and respect for diversity as well as religious and ethical values. The WPAY focuses on 15 priority areas, among which is juvenile delinquency. Under that priority area, it details proposals for action towards preventing juvenile delinquency and rehabilitating young people who have engaged in criminal activity.

The primary goals of the juvenile justice system, in addition to maintaining public safety, are skill development, habilitation, rehabilitation, addressing treatment needs, and successful reintegration of youth into the community. The juvenile justice system takes a significantly more restorative approach than the adult criminal justice system. A truly successful case for youth would result in the adolescent learning from the experience without exposure to the severity of an adult prison, altering their decisions and life course moving forward, and having no future contact with the juvenile or criminal justice systems.

Legal terms :

Juvenile justice	قضاء الاحداث
the policies, strategies	السياسات، الاستراتيجيات
Laws, procedures and practices	القوانين، الاجراءات والممارسات
criminal responsibility	المسؤولية الجنائية
Conflict with the law	مخالفة(انتهاك) للقانون
Justice for children	العدالة للاطفال
victims or witnesses of crime	ضحايا أو شهود عن الجريمة
justice system	نظام العدالة
Custody	الحضانة
Protection	الحماية
Inheritance	الميراث
Convicted of a criminal offence	المدان بارتكاب جرائم
The United Nations Rules for the Protection	قواعد الامم المتحدة لحماية الاحداث المجردين من الحرية

of Juveniles Deprived of their Liberty	
The United Nations Standard Minimum Rules for the Administration of Juvenile Justice	قواعد الأمم المتحدة النموذجية الدنيا لإدارة شؤون قضاء الأحداث
The Committee on the Rights of the Child (CRC	لجنة حقوق الطفل
Guidelines	المبادئ الارشادية
engaging in criminal activities	الذين شاركوا في النشاطات الاجرامية
Convention on the rights of child(CRC)	اتفاقية حقوق الطفل
Entred into force	دخلت حيز النفاذ
adopted the World Programme of Action for Youth (WPAY)	تبنت برنامج العمل العالمي للشباب
policy framework	الاطار العام للسياسة
Practical guidelines	مبادئ إرشادية عملية
national action	العمل الوطني
international support	الدعم الدولي
Governments	الحكومات
violations of all human rights and fundamental freedoms	انتهاكات حقوق الانسان والحريات الاساسية
promote non-discrimination	تعزيز عدم التمييز
Tolerance	التسامح
respect for diversity	احترام الاختلاف
religious and ethical values	القيم الدينية والاخلاقية
preventing juvenile delinquency	منع جنوح الاحداث
rehabilitating young people	اعادة تاهيل الشباب
maintaining public safety	حفظ الامن العام
Habilitation	التاهيل
Rehabilitation	إعادة التاهيل
reintegration of youth	اعادة إدماج الشباب
Adult criminal justice system	نظام العدالة الجنائية للبالغين
Decisions	القرارات

قضاء الاحداث

قضاء الاحداث او كما يشار اليه حسب المبادي الارشادية عدالة الاحداث أو عدالة الاطفال هو مصطلح عام يستخدم للتعبير عن السايسات، الاستراتيجيات، القوانين، الاجراءات والممارسات المطبقة على الاطفال الذين تجاوزوا الحد الادنى للمسؤولية الجنائية والذين يخالفون القانون، ويجب تمييزه عن المفهوم الواسع " العدالة للاطفال" والذي يشمل الاطفال الذين خالفوا القانون (أي من يدعى انهم، او متهمون او ثبت انتهاكهم لقانون العقوبات)، الاطفال الضحايا او الشهود عن الجرائم، والاطفال الذين يمكن ان يكونوا على اتصال مع نظام العدالة لأسباب أخرى مثل الحضانة، الحماية أو الميراث . ورغم عدم وجود تعريف مقبول لمصطلح الحدث فعادة ما يستخدم للاشارة الى الاطفال الذين تجاوزوا السن الادنى للمسؤولية الجنائية وهم مدعى انهم، او متهمون، أو تمت ادانتهم بالجرائم.

تعرف قواعد الامم المتحدة لحماية الاحداث المجردين من الحرية (قواعد هافانا) الحدث بانه كل شخص دون سن الثامنة عشر، أما قواعد الأمم المتحدة النموذجية الدنيا لإدارة قضاء الأحداث (قواعد بكين) فتعرفه كالتالي: "الحدث هو طفل او شاب يمكن التعامل معه بموجب نظام قانوني معين عند ارتكابه لجريمة ما بطريقة تختلف عن الشخص البالغ ".

بينما تتجنب لجنة حقوق الطفل استخدام مصطلح الحدث وتستبدله بعبارة الاطفال المخالفين للقانون.

لقد وضعت قواعد بجين والمبادئ الارشادية للرياض اجراءات أساسية لمنع الاطفال والشباب من الاشتراك في النشاطات الاجرامية وحماية حقوق الشباب الذين ثبت انتهاكهم للقانون. فقي 1989 تعزز التركيز على حقوق الانسان للطفل والشباب من خلال اتفاقية حقوق الطفل، التي دخلت حيز النفاذ عام 1990.

وفي عام 1995 تبنت الامم المتحدة برنامج العمل العالمي للشباب، والذي يوفر اطارا عاما للسياسة ومبادئ ارشادية عملية للعمل الوطني والدعم الدولي لتحسين وضعية الشباب .

من خلال هذا البرنامج، وضعت الامم المتحدة سياسة عمل مصممة خصيصا للشباب مابين 15 و 24 سنة، و يهدف هذا البرنامج الى تعزيز الظروف والاليات لتحسين رفاه وسبل العيش بين الشباب، وعلى هذا النحو، فهو يتطلب من الحكومات اتخاذ اجراءات فعالة ضد انتهاكات حقوق الانسان والحريات الاساسية ، ولتعزيز عدم التمييز، التسامح واحترام التنوع والقيم الدينية والاخلاقية، حيث يركز هذا البرنامج على 15 أولوية من بينها قضاء الاحداث، وضمن هذه الأولوية

يقدم مقترحات مفصلة للعمل من أجل منع جنوح الأحداث، وإعادة تأهيل الشباب الذين شاركوا في نشاط إجرامي.

إن الأهداف الأساسية لنظام قضاء الأحداث، بالإضافة إلى الحفاظ على السلامة (الأمن) العامة تتمثل في تنمية المهارات، التأهيل إعادة التأهيل، معالجة الاحتياجات العلاجية، و إعادة الإدماج الناجح للشباب في المجتمع.

يتبع نظام قضاء الأحداث مقاربة إصلاحية بشكل كبير مقارنة بنظام العدالة الجنائية للبالغين، فنجاح أي قضايا الشباب سيؤدي إلى تعلم المراهقين من التجارب دون التعرض لخطورة سجن البالغين، وتغيير قراراتهم، ومسار حياتهم للمضي قدما، وعدم الاتصال مستقبلا مع أنظمة الأحداث أو أنظمة العدالة الجنائية.

Master 2/ criminal law

Text N°: 04

Criminal proof

The law of criminal evidence governs how parties, judges, and juries offer and then evaluate the various forms of proof at trial. In some ways, evidence is an extension of civil and criminal procedure. Generally, evidence law establishes a group of limitations that courts enforce against attorneys in an attempt to control the various events that the trial process presents in an adversarial setting.

There are many arguments in favor of evidence law. Here are five of the most common ones:

1. To ameliorate pervasive mistrust of juries
2. To further legal or social policies relating to a matter being litigated
3. To further substantive policies unrelated to the matter in suit
4. To create conditions to receive the most accurate facts in trials
5. To manage the scope and duration of trials.

The outcome of many criminal law cases will depend upon the strength and admissibility of evidence -- including physical proof, scientific evidence, and witness testimony. Criminal evidence law can be complex, but we will evoke the sense of the different rules and concepts surrounding evidence, as admissibility, witness testimony, the use of scientific evidence in court…..etc

Admissible Evidence

In order to be admitted at court, Evidence must be relevant, material, and competent. To be relevant evidence must reasonably help prove or disprove some fact. The degree to which this evidence increases or decreases the likelihood of the fact for which it was introduced will influence the weight it is given by the judge or jury. Evidence is material if it is offered to prove a fact in dispute and it is competent if it falls within certain standards of reliability.

Suppressed Evidence

Evidence that might otherwise be admitted in a criminal case can be suppressed when it has been illegally obtained. Evidence produced as a result of an unlawful search and seizure, , or evidence for which the chain of custody is broken may all be suppressed. Any evidence produced as the result of these flawed circumstances may also be suppressed." Evidence that would normally be suppress-able may still be admitted where it would have inevitably been

discovered, the officer was acting on good faith, or when an independent source would have produced the same evidence.

Scientific and Forensic Evidence

There are many kinds of scientific evidence admitted to criminal courts including fingerprints, fiber analysis, DNA and other evidence. Any scientific evidence produced at trail must first be shown to be established within the scientific community and generally accepted as true before it can be asserted at trial. Fingerprint and DNA matching are reasonably well-understood, but there are times when less established kinds of scientific evidence are introduced. When necessary a hearing on the validity of a scientific theory takes place prior to the trial on the merits of the principal case.

Legal terms :

Criminal proof	الاثبات الجنائي
law of criminal evidence	قانون الادلة الجنائية
To govern	تحكم(تنظم)
Forms of proof	اشكال الاثبات
A trial	المحاكمة
Civil and criminal prpcedure	الاجراءات المدنية والجزائية
Trial process	عملية المحاكمة
Evidence law	قانون الادلة
legal or social policies	السياسات القانونية والاجتماعية
a matter being litigated	مسالة محل تقاضي(محل نزاع)
substantive policies	السياسات المادية
Suit(lawsyuite)	الدعوى
admissibility of evidence	مقبولية الدليل
physical proof	الاثبات المادي
scientific evidence	الدليل العلمي
witness testimony	شهادة الشهود
Admissible evidence	الدليل المقبول
prove or disprove	اثبات او دحض
Fact (facts)	حقائق(وقائع)
standards of reliability	معايير الموثوقية
Suppressed evidence	الدليل الملغى
Criminal case	القضية الجنائية
illegally obtained	المحصل عليه(ها) بطريقة غير قانونية
unlawful search and seizure,	البحث والحجز الغير قانونيين
Character evidence	الادلة الشخصية
To be guilty	ان يكون مدانا
To prove gyuilt	لاثبات الادانة
leniency or strictness in punishment	تخفيف او تشديد العقوبة
Civil suit	الدعوى المدنية
Similar rules	قواعد مماثلة
Scientific and Forensic Evidence	الادلة العلمية والشرعية
fingerprints, fiber analysis, DNA	البصمات، تحاليل الالياف، الا دي ان

جلسة استماع	Hearing

الادلة الجنائية

يحكم قانون الاثبات الجنائي كيفية تقسيم وتقييم الاطراف، وهيئة المحلفين لمختلف أشكال الاثبات في المحاكمة من بعض النواحي، يعد الاثبات امتدادا للاجراءات المدنية والجزائية، وعموما يضع قانون الاثبات مجموعة من القيود التي تفرضها المحاكم ضد المحامين في محاولة للسيطرة على مختلف الاحداث التي تعرضها عملية المحاكمة في سياق الخصومة.

حجج ومبررات قانون الاثبات:

التخفيف من انعدام الثقة السائد في هيئات المحلفين.

تعزيز السياسات القانونية والاجتماعية المتعلقة بالمسألة المعروضة على التقاضي (محل النزاع).

تعزيز السياسات الموضوعية التي ليس لها صلة بالموضوع في الدعوى.

خلق ونهيئة شروط لتلقي واستقبال ادق الحقائق(الوقائع) في المحكمة.

تسيير وادارة نطلق ومدة المحاكمة

ستعتمد نتائج العديد من قضايا القانون الجنائي على قوة ومقبولية الادلة سيما في ذلك الدليل المادي، الدليل العلمي وشهادة الشهود.

يمكن ان يكون قانون الاثبات الجنائي معقدا، لكننا سنتطرق الى معنى مختلف القواعد والمفاهيم المتعلقة بالاثبات مثل المقبولية، شهادة الشهود، استخدام الادلةة في المحمكمة.....الخ.

1-الادلة المقبولة:

بهدف قبولها في المحكمة يجب ان تكون الادلة ذات صلة(مرتبطة)، مادية ومتخصصة، فحتى تكون ذات صلة يجب ان تساعد بشكل معقول في اثبات او دحض بعض الوقائع ، وتؤثر الدرجة التي يزيد بها هذا الدليل او ينقص من احتمالية الحقيقة(الواقعة) التي تم تقديمها على الوزن الذي يمنحها القاضي أو هيئة المحلفين.

تكون الادلة مادية اذا ما تم تقديمها لاثبات حقيقة متنازع عليها، وتكون متخصصة اذا ما اندرجت ضمن معايير معينة من الموثوقية.

2-الادلة الملغاة

يمكن الغاء الادلة المقبولة في القضايا الجنائية متى تم الحصول عليها بطريقة غير قانونية، فالدليل المقدم كنتيجة لبحث وحجز غير قانونيين ، والادلة التي من اجلها تم كسر سلسلة الحراسة، وكل دليل يقدم نتيجة ظروف معيبة يجب الغاؤه.

إن الدليل الذي يمكن الغاؤه يجب أن يبقى مقبولا طالما تم اكتشافه حتما وان الضابط كان قد تصرف بحسن نية أو كان المصدر المستقل يتيح نفس الادلة.

3-الادلة العلمية والشرعية: هناك العديد من أنواع الأدلة المقبولة أمام المحاكم الجزائية بما فيها البصمات، تحليل الالياف، الا دي ان وأدلة أخرى...، فكل دليل علمي يقدم أمام المحاكمة يجب إثبات انه معترف به في المجتمع العلمي ومقبول على العموم تحقيقه قبل ان يتم الاستشهاد به أمام المحاكمة، فمطابقة البصمات والا دي ان تكون مفهومة ومقبولة بشكل جيد، لكن أحيانا يتم تقديم بعض أنواع الأدلة العلمية الأقل رسوخا وعند الضرورة تعقد جلسة استماع حول صحة النظرية العلمية من قبل المحكمة في القضية الرئيسية.

Master 2/ criminal law

Text N°: 05

Juvenile Delinquency

Juvenile delinquency, also known as **juvenile offending**, is the act of participating in unlawful behavior as a minor or individual younger than the statutory age of majority.

Or it's a term used to describe illegal actions by a minor. This term is broad in range and can include everything from minor violations like skipping school to more severe crimes such as burglary and violent actions.

Understanding why a minor commits a crime is essential to preventing future crimes from happening. Addressing the issues that has led to the choices that the minor child has made can help them change their actions in the future.

By addressing many of these issues at an early age, adults may be able to stop juvenile delinquency from starting. If delinquency has already occurred, addressing these issues and building protective barriers may allow the child to develop in a more secure environment and avoid problems in the future as well as when they are adults.

Leading Contributing Factors To Juvenile Delinquency:

Poor School Attendance: it is one of the top factors contributing to delinquency. School is not only a place to learn and grow; it is also a structured routine that provides children with a goal to accomplish each day**.**

Children who are not encouraged to learn this type of routine are losing out on establishing good habits. They are also experiencing a lot of free time that can be used to "learn" about other things that will not enhance their lives or their futures.

Poor Educational Standards : The type of school that a child attends may also contribute to their delinquency. Overcrowded and underfunded schools tend to lack discipline and order. The chaos often experienced in these schools lead children to act more defensively.

Parental involvement in school work and school activities has been found to be a very large deterrent for delinquent activities.

Violence In The Home: One of the largest contributing factors to delinquency is violence in the home Lashing out at others for the violence they experience at home is very common. Teens subjected to violent actions, or those who witness it to others, are more likely to act**.**

Violence In Their Social Circles: If the neighborhood is in which a child lives is violent, the children will have a tendency to be more prone to delinquency.

In many ceses, when you remove the child from this type of situation, their tendency for delinquent actions is removed.

Socioeconomic Factors : Juvenile delinquency is more common in poorer neighborhoods. While all neighborhoods are not exempt from delinquent activities, it is believed they happen more in areas where children feel they must commit crimes to prosper.

Theft and similar crimes may actually be a result of necessity and not that of just a petty crime.

Lack Of Moral Guidance: Parental or adult influence is the most important factor in deterring delinquency. When a parent or other adult interacts with the child and shows them what is acceptable behavior and what is considered wrong, the child is more likely to act in a way that is not delinquent**.**

It is very important for a child to have a bond with a good adult who will influence their actions and show them the difference between what is right and what is wrong.

Legal terms

Juvenile delinquency(juvenile offending**)**	جنوح الاحداث
Inlawful behavior	السلوك الغير مشروع
A minor	قاصر
Statutory age of majority	سن الرشد القانوني
Illegal actions	اعمال غير مشروعة
Burglary and violent actions	أعمال السطو والعنف
Adressing issues	معالجة القضايا
Protective bariers	الحدود (الحواجز الحمائية)
More secure environment	بيئة اكثر أمنا
Discipline and order	الانضباط والنظام
A deterrent	رادع
Regular bases	اسس نظامية
deterring delinquency	ردع الانحراف

جنوح الأحداث

يعني جنوح الأحداث مساهمة القصر أو من هم اقل من سن الرشد القانوني في السلوكات الغير شرعية. كما يستعمل هذا المصطلح بشكل واسع في التعبير عن الانتهاكات او المخالفات البسيطة مثل التغيب المدرسي إلى جرائم أكثر خطورة كأعمال السطو والعنف وأعمال العنف.

إن فهم أسباب ارتكاب القاصر للجريمة يعد أمرا ضروريا للوقاية من الجرائم المستقبلية، فمعالجة القضايا الذي أدت إلى هذه الاختيارات من طرف القاصر يمكن ان تساعد في تغيير هذه الأفعال مستقبلا. كما أن معالجتها في وقت مبكر تمكن الكبار من التوقف عن جنوح الأحداث منذ البداية، أما إذا وصلنا إلى مرحلة الجنوح فان معالجة هاته المسائل ووضع حواجز حمائية يمكن أن تسمح للطفل بالتطور في بيئة أكثر أمنا، وتجنبه المشاكل مستقبلا وكذا الشأن بالنسبة للبالغين.

العوامل الرئيسية المساهمة في جنوح الأحداث:

-**ضعف الحضور الى المدرسة**: ويعتبر من أهم العوامل المساهمة في الجنوح، فالمدرسة ليست مكانا للتعلم والنمو فقط بل هي الروتين المنظم الذي يزود الأطفال بالأهداف الواجب تحقيقها كل سنة .

فالأطفال الذين لم يتلقوا التشجيع في فهم هذا الروتين لا يمكنهم وضع وتأسيس عادات جيدة، حيث يعانون من وقت فراغ كبير من المفروض انه سيستغل في دفع حياتهم قدما.

-**معايير التعليم الضعيفة**: والذي يمكن ان يسهم في جنوح الأحداث، فالمدارس المكتظة والغير ممولة جيدا تميل الى فقدان الانضباط والنظام، وعادة ما تؤدي الفوضى السائدة في هذا النوع من المدارس تصرف الأطفال بطرق اندفاعية بسبب خوفهم من محيطهم.

كما أن إشراك الا ولياء في الأعباء ومختلف الأنشطة المدرسية يعد رادعا قويا ضد الجنوح.

العنف في المنزل: إن العنف في المنزل ومن خلال الانتقادات الموجهة للاخرين أمر جد شائع، فالمراهقون الذين تعرضوا لإعمال العنف أو من كانوا شهودا عليها من المحتمل جدا أن يتصرفوا كذلك.

العنف في الدائرة (المحيط) الاجتماعي: فإذا كان الاطفال يعيشون في احياء تشهد العنف فسيكون لهم ميول لان يكونوا اكثر عرضة للجنوح. وفي كثير من الحالات فان ابعاد الاطفال عن مثل هذه الوضعيات سيبعدهم عن الاعمال المنحرفة.

العوامل السوسيو اقتصادية: حيث يكون جنوح الاحداث اكثر انتشارا في الاحياء الفقيرة، فكل الاحياء ليست بمنأى عن هذه النشاطات المنحرفة، وتنتشر أكثر في المناطق التي يشعر فيها الاطفال بضرورة ارتكابهم لهذه الافعال للاحساس بالازدهار. وتكون بذلك السرقة والجرائم المماثلة لها فعليا هي نتيجة الحاجة وليست نتيجة جرائم بسيطة.

غياب التوجيه الاخلاقي:
يعتبر تأثير الوالدين أو الكبار العامل الأكثر أهمية في ردع الانحراف. فعندما يتفاعل أحد الوالدين أو أي شخص بالغ آخر مع الطفل ويظهر له ما هو السلوك المقبول وما هو السلوك الخاطئ، فيكون من المرجح أن يتصرف الطفل بطريقة غير منحرفة. فمن المهم جدًا أن يكون للطفل علاقة مع شخص بالغ جيد يؤثر على أفعاله ويظهر له الفرق بين ما هو صواب وما هو خطأ.

Master 2/ criminal law

Text N°: 06

Penal Reform

The Algerian constitution states that anyone charged with a crime is presumed innocent until proven guilty. It also recognizes the right of the accused to a lawyer and guarantees the right to defense in penal matters. However, the right to a fair trial is frequently undermined by the use of confessions under duress to produce convictions. Detainees suspected of serious crimes are routinely denied access to a lawyer, often held incommunicado, and prevented from contacting family members— all in violation of the penal code.

Preventive detention is still widely practiced. The code of penal procedures empowers authorities to detain a suspect for up 48 hours before arraignment by an examining magistrate.

Poor conditions prevail in Algeria's prisons : Most of the prisons were built during the French colonial period and are in a state of dilapidation, with lack of space and inadequate premises. Prisons are overcrowded because imprisonment is the main sentence used and very few alternatives are available. Although Algeria is one of the rare countries in the region with a permanent school for its prison staff, the training curriculum and the methods used require a thorough review and modernization.

Algeria has taken steps to amend its laws and penal code to place them in conformity with international human rights conventions. It has not carried out capital punishment since 1994 and has indicated its intention to eliminate the death penalty. In October 2004, the government passed a new Penal Code legislation criminalizing torture for the first time. On request of the Algerian government, Penal Reform International (PRI), an international NGO, began to work in the country in January 2002. The government asked PRI for support in its forthcoming justice reform process, including the penal and prison systems. A common project was swiftly drawn up based on the needs and priorities identified by the Algerian General Prison and Rehabilitation Direction (AGPRD). PRI's work comprises three main parts: **prison staff training** (for prison directors, technical professionals, such as doctors, psychologists, social workers and staff working not only but mainly with juvenile delinquents) and training of trainers programs to strengthen the Algerian prison staff training institutions. **training of magistrates** and the promotion of alternatives to custody, and three: **facilitating detainee rehabilitation** through the development of classes and vocational and skills-training workshops inside the prisons.

Since 2002, the following procedures to improve and modernize the penal and prison system have been created through the assistance of PRI:

• the central prison administration has been reorganized;

• requirements for the selection of prison staff, especially in terms of education, have been raised;

• the duration of initial training has been extended;

• rehabilitation has been officially introduced in the initial prison staff training curriculum;

• a large campaign of prison staff recruitment has been launched, with its emphasis on specific categories such as psychologists, doctors, social workers, and sports trainers;

• agreements have been signed with various ministries to improve the quality of services for prisoners, such as education • partnerships with national NGOs have been initiated

• a new Prison Code confirming a complete change of approach and real and fundamental progress towards better respect for prisoner's rights has been adopted.

Legal terms :

Penal reform	الاصلاح العقابي
Constitution states	ينص الدستور
Proven guilty	اثبات الادانة
the right of the accused to a lawyer	حق المتهم في الاستعانة بمحام
the right to defense in penal matters	حق الدفاع في المسائل الجنائية
The right to a fair trial	الحق في محاكمة عادلة
Duress	الاكراه
Convictions	الاثبات
Detainees suspected	المحتجزين المشتبه بهم
access to a lawyer	الاستعانة بمحام
Violation of the penal code	مخالفة او انتهاك لقانون العقوبات
Preventive detention	الحبس الاحتياطي
The code of penal procedures	قانون الاجراءات الجزائية
Authorities	السلطات
to detain a suspect	حجز المشتبه به
An examining magistrate	قاضي التحقيق
Suspected terrorists and subversives	الارهابيون والمخربون المشتبه بهم
prison staff	موظفي السجون
International human rights conventions	الاتفاقيات الدولية لحقوق الانسان
carriy out capital punishment	تنفيذ عقوبة الاعدام
Elimination of death penalty	الغاء عقوبة الاعدام
Penal Code legislation criminalizing torture	تشريع قانون عقوبات يجرم التعذيب

Penal Reform International	الاصلاح الجنائي الدولية
an international NGO,	منظمة غير حكومية دولية
justice reform process	عمليات (مسار اصلاح العدالة)
Penal and prison systems	انظمة العقاب والسجون
Algerian General Prison and Rehabilitation Direction (AGPRD)	المديرية العامة للسجون واعادة الادماج
prison staff training	تدريب موظفي السجون
Magistrate training	تدريب القضاة
the promotion of alternatives to custody	ترقية بدائل للحبس
facilitating detainee rehabilitation	تسهيل اعادة ادماج المحبوسين
the central prison administration	الادارة المركزية للسجون
Procedures	الاجراءات
requirements for the selection of prison staff	متطلبات انتقاء موظفي السجون
Agreements	اتفاقات
national NGOs	المنظمات الغير حكومية
Prison Code	قانون السجون
prisoner's rights	حقوق المساجين
has been adopted	تم تبنيه (اعتماده)

الاصلاح العقابي

ينص الدستور الجزائري على انه يعد بريئا كل شخص ارتكب جريمة الى غاية اثبات ادانته، كما يعترف أيضا بحق المتهم في الاستعانة بمحام، ويضمن له حق الدفاع في القضايا او المسائل الجنائية، غير أنه عادة ما يتم تقويض الحق في المحاكمة العادلة من خلال استخدام الاعتراف وتحت الاكراه للحصول على أدلة للادانة، كما أن المحتجزين المشتبه بهم في الجرائم الخطيرة عادة ما لا يسمح بهم بالاستعانة بمحام، حيث يتم الاحتجاز بمعزل عن العالم الخارجي كما يحرمون من الاتصال باسرهم، وهذا مايشكل انتهاكا لقانون العقوبات.

فلا يزال الحبس الاحتياطي يمارس بشكل واسع، إذ يجيز قانون الاجراءات الجزائية للسلطات حجز المشتبه بهم لمدة تصل الى ثمانية واربعين ساعة قبل استدعائهم الى المحكمة من طرف قاضي التحقيق.

الظروف السيئة السائدة في السجون الجزائرية:

حيث تم انشاء أغلبها أثناء الاستعمار الفرنسي، وهي في حالة جد سيئة، مع ضيقها وعدم كفايتها اضافة الى اكتضاضها لأن السجون من أهم الوسائل المستخدمة، و ان البدائل المتاحة جد قليلة، كما أن الجزائر من الدول القليلة في المنطقة التي تتوفر على مدرسة دائمة للمساجين، إضافة الى حاجة عمليات التدريب والنماذج المستخدمة الى المراجعة والتحديث الشامل، غير أن الجزائر قد خطت خطوات في مجال تعديل قوانينها وخاصة قانونها الجنائي لجعله يتطابق مع اتفاقات حقوق الانسان، إذ لم تنفذ عقوبة الاعدام منذ عام 1994 ، كما أعلنت عن رغبتها في القضاء على عقوبة الاعدام، وفي اكتوبر 2004 مررت الحكومة تشريع قانون عقوبات يجرم التعذيب لاول مرة، وبطلب من الحكومة الجزائرية بدأت

المنظمة الغير حكومية الدولية (الاصلاح الجنائي الدولية)(PRI) بدأت عملها في الجزائر في جانفي 2002، حيث طلبت الحكومة الدعم من المنظمة من أجل مسار الاصلاحات المستقبلية للعدالة بما في ذلك في الانظمة العقابية وانظمة السجون.

كما تم وضع مشروع مشترك قائم على الحاجات والأولويات المحددة من طرف المديرية العامة للسجون وإعادة الادماج (AGPRD) فعمل منظمة الاصلاح الجنائي الدولية يشمل ثلاثة محاور:

- تدريب موظفي السجون(مديري السجون، الاخصائيين الممارسين مثل الاطباء، والاخصائيين النفسانيين، والاجتماعيين، وللموظفين العاملين اساسا مع الاحداث الجانحين برامج تدريب لتعزيز وتقوية مؤسسات تدريب موظفي السجون الجزائرية.

-تدريب القضاة وترقية بدائل للرقابة.

-تسهيل إعادة إدماج المساجين من خلال تطوير اقسام وورشات عمل مهنية والتدريب على المهارات داخل السجون.

منذ 2002 ، وبمساعدة من منظمة الاصلاح الجنائي الدولية تم وضع مجموعة من الاجراءات لتحيين وعصرنة المنظومة العقابية وانظمة السجون تمثلت فيما يلي:

-اعادة تنظيم الادارة المركزية للسجون.

-الرفع من متطلبات اختيار موظفي السجون خاصة في مجال التعليم.

-تمديد مدة التدريب الابتدائي.

-ادخال اعادة الادماج رسميا في منهج التدريب الاولي للمساجين

- إطلاق حملة توظيف في السجون مع التركيز على الفئات الخاصة مثل الاخصائيين النفسانيين، الاطباء، الاخصائيين الاجتماعيين، ومدربي الرياضة.

-التوقيع على العديد من الاتفاقيات مع مختلف الوزارات لتحسين نوعية الخدمات لفائدة المساجين مثل التعليم، مبادرات الشراكة مع المنظمات غير الحكومية الوطنية.

-اعتماد قانون جديد للسجون الذي يؤكد التحول الشامل للمقاربة والتطور الفعلي والأساسي اتجاه احترام حقوق المساجين.

Master 2/ criminal law

Text N°: 07

Electronic evidence and its authenticity in forensic evidence (part1)

Computer and information technology crimes are varied and there are numerous ways to perpetrate them, which makes it difficult for investigators to provide evidence of these crimes. Legal authorities must search for new evidence from crime scenes, especially perpetrators of the crime.

Cybercrimes are among the most serious criminal activity of the present day; they threaten the progress that the world has reached using the Internet in all areas of life, and they weaken confidence in its use as a quick, easy, and safe tool. It can be difficult to prove when a cybercrime is committed, making it difficult for investigators to find evidence through which the crime can be proven and its perpetrators can be convicted.

The field of computer forensics is still new, and challenging, and cybercrime requires specialized technical expertise in order to search for evidence. It is very difficult for investigators to prove these crimes because the evidence is quickly and easily erased. Delays caused by the authorities' lack of experience collecting cyber evidence, investigating, and bringing suspects to trial may result in the loss of evidence.
Modern researches concerning the issues of electronic evidence in forensic science and criminal procedure are devoted to such issues as the preservation of digital evidence and its admissibility in the court, the role of electronic evidence in the detection and investigation of cybercrimes, classification and evaluation of digital forensic tools, opportunities and challenges for electronic evidence.
The challenges encountered are the nature of information technology crimes represented in computers and the Internet, the procedures for proving them, the validity and integrity of the electronic evidence, and the validity of the evidence extracted from the electronic tool in criminal evidence. Electronic crimes have a special nature due to the gravity of their offense, the enormity of their losses, their increasing numbers, and how easy it is to commit them. There is also a problem related to the extent of the judge's discretionary powers in assessing the evidence extracted from electronic means.

Kinds of forensic evidence are many including physical or documentary, or eyewitness testimony. Forensic electronic evidence is submitted to prove a crime occurred using a computer and the Internet. This evidence is retrieved using information technology.
Electronic crimes are committed in a space that has no use for papers or hard copies, but rather a virtual world related to computer technology and the Internet. This makes it easier for a perpetrator to tamper with data and programs moments after committing a crime, thus obliterating any evidence. This makes it difficult for investigators to collect proof.
Due to the great and rapid development of computer technology and the Internet, new types of crime have emerged. Such crimes are diverse and criminals use various methods to commit them. Then, due to the speed electronic crimes are committed, and the easy erasure of their evidence, it has become difficult to obtain, identify, and classify evidence. This makes it difficult for investigators to prove crimes were committed, and take the accused to trial.
The general rule in criminal cases pending before the courts is that they may be proven by all legally acceptable methods of evidence.
One result of the development in methods for collecting evidence may be impunity of the perpetrators if evidence for the commission is not found.
Obtaining evidence from information technology systems raises many difficulties for investigators for several reasons. Additionally, there is the ease of quickly erasing or manipulating digital evidence. Before the introduction of digital technologies into widespread use, forensic techniques, and methods were based on previous developments based on the study of the material world. The authorities in charge of the investigation were accustomed to evidence being tangible, but the virtual world is different, and the investigator cannot apply traditional evidence procedures to crimes committed in that world. Rather, investigators need specialized technical expertise and training to search for evidence, such as examining hard drives and other electronic tools and systems.

Legal terms :

To perpetrate crimes	ارتكاب الجرائم

Investigators	المحققون
To provide evidence	توفير (تقديم) الدليل
Legal authorities	السلطات القانونية
serious criminal activity	النشاطات الاجرامية الخطيرة
Threaten	تهدد
Weaken confidence	تضعف من السرية
the crime can be proven	يمكن اثبات الجريمة
perpetrators can be convicted	يمكن إدانة الفاعلين (مرتكبي الجريمة)
bringing suspects to trial	إحالة المشتبه بهم إلى المحاكمة
The issues of electronic evidence	مسائل الاثبات الالكتروني
forensic science	العلوم الجنائية (الشرعية)
criminal procedure	الاجراء الجنائي
are devoted	مكرسة
the preservation of digital evidence	الحفاظ على الدليل الالكتروني
its admissibility in the court	مقبوليته أمام المحكمة
the detection and investigation of cybercrime	الكشف والتحري حول الجريمة السيبيرانية
classification and evaluation of digital forensic tools	تصنيف وتقييم الدليل الرقمي
Opportunities and challenges	الفرص والتحديات
the procedures for proving	اجراءات الاثبات
The validity and integrity of the electronic evidence	صلاحية وسلامة الدليل الالكتروني
Criminal evidence	الادلة الجنائية
the judge’s discretionary powers	السلطات التقديرية للقاضي
assessing the evidence	تقدير الدليل
Forensic evidence	الادلة الشرعية
physical or documentary, or eyewitness testimony	المادي أو المستندي، أو شهادة الشهود
Perpetrator	الفاعل، مرتكب الجريمة
to tamper	التلاعب

to collect proof.	جمع الادلة
Criminals	المجرمين
To commit	ارتكاب
take the accused to trial	احالة المتهم الى المحاكمة
The general rule	القاعدة العامة
criminal cases pending	القضايا الجنائية قيد الانتظار
they may be proven by all legally acceptable methods of evidence	الممكن اثباتها بكل وسائل الاثبات المقبولة قانونا
impunity of the perpetrators	افلات المجرمين من العقوبة
evidence for the commission	دليل ارتكاب
manipulating digital evidence	التلاعب بالدليل الرقمي
The authorities in charge of the investigation	السلطات (الهيئات) المكلفة بالتحقيق
evidence being tangible	الادلة الملموسة
traditional evidence procedures	اجراءات الاثبات التقليدية
Examining	فحص

الدليل الالكتروني وحجيته في الاثبات الجنائي (الجزء 1)

تتنوع جرائم الكمبيوتر وتكنولوجيا المعلوماتية وتتعدد طرق ارتكابها، مما يصعب على جهات التحقيق تقديم أدلة حولها، إذ يجب أن تبحث السلطات القانونية عن الادلة من مسرح الجريمة، وعن مرتكبيها على وجه الخصوص.

تعتبر الجرائم السيبيرانية من بين أهم النشاطات الاجرامية الخطيرة في وقتنا الحالي، فهي تهدد التقدم الذي يشهده العالم من خلال استخدام الانترنت في كل مجالات الحياة، كما تضعف من السرية من حيث استعمالها كوسيلة سهلة، سريعة وآمنة، كما يمكن أن يكون من الصعب اثبات متى تم ارتكاب الجريمة، مما يصعب على المحققين ايجاد أدلة التي يمكن خلالها اثبات هذه الجرائم وادانة مرتكبيها.

يعتبر مجال علوم الكمبيوتر مجالا حديثا ويثير العديد من التحديات، كما تتطلب الجرائم السيبيرانية خبرات تقنية متخصصة من أجل البحث عن الدليل، فيكون من الصعب على جهات التحقيق اثبات هذه الجرائم بسبب سهولة وسرعة ازالة ومحو الدليل، إضافة إلى التأخر الناجم عن نقص وانعدام خبرة السلطات في جمع الادلة الرقمية، والتحقيق فيها، كما أن احالة المشتبه بهم الى المحاكمة يمكن ان ينتج عنه فقدان الدليل.
لقد كرست الابحاث الحديثة اهتماماتها بقضايا الاثبات الالكتروني في العلوم الجنائية والاجراءات الجزائية على غرار الحفاظ على الادلة الرقمية، ومقبوليتها أمام المحاكم، ودور الأدلة الالكترونية في الكشف والتحقيق بشأن الجرائم الالكترونية، تصنيف وتقييم الوسائل الرقمية العلمية، فرص وتحديات الادلة الالكترونية.
من أبرز التحيات المثارة نجد طبيعة جرائم تكنولوجيا المعلوماتية التي تتم عبر الحواسيب والانترنت، وكذا اجراءات إثباتها، صحة وسلامة الادلة الالكترونية، وصحة الدليل المستخرج من الوسائل الالكترونية في الاثبات الجنائي.
للجرائم الالكترونية طبيعة خاصة بسبب خطورتها، وحجم خسائرها، وعددها المتزايد، وسهولة ارتكابها، إضافة إلى مسألة أو مشكلة امتداد السلطة التقديرية للقاضي بشأن تقدير الادلة المستخرجة من الوسائل الالكترونية.
تتعدد أنواع الادلة الجنائية بما فيها المادية، المستندية أو شهادة الشهود، وتستعمل الأدلة الالكترونية العلمية في إثبات الجرائم المرتكبة باستخدام الكمبيوتر والانترنت، وتسترجع هذه الأدلة باستخدام تكنولوجيا المعلومات.

وترتكب الجرائم السيبيرانية في فضاءات تستغني عن الورق والنسخ الورقية، بل في عالم افتراضي يرتبط بتكنولوجيا الحاسوب والانترنت، مما يسهل على مرتكبها التلاعب بالبيانات والبرامج في ظرف لحظات من ارتكابها، مما يطمس (يزيل) كل دليل، وهو ما يصعب على المحققين جمع الأدلة، ونظرا للتطور الكبير والسريع لتكونولوجيا الإعلام والانترنت، برزت جرائم جديدة، بإمكان مرتكبيها استخدام وسائل متنوعة في ارتكابها، وبسبب سرعة ارتكابها وسهولة إزالة ومحو الأدلة أصبح من الصعب الحصول على الأدلة، تحديدها وتصنيفها. مما يصعب في النهاية على جهات التحقيق إثبات ارتكابها وإحالة المتهمين الى المحاكمة.

إن القاعدة العامة في المسائل الجنائية قيد الانتظار أمام المحاكم هي إمكانية إثباتها بكل وسائل الإثبات المقبولة قانونيا، ومن نتائج تطور طرق ووسائل جمع الأدلة إمكانية إفلات الفاعلين إذا لم يوجد دليل على ارتكابهم لهذه الجرائم، إن الحصول على الأدلة من أنظمة تكنولوجيا المعلومات يثير العديد من الصعوبات في وجه المحققين نتيجة للعديد من الأسباب، بالإضافة إلى الأدلة الرقمية، وقبل إدخال التكنولوجيا الرقمية واستعمالها الواسع، كانت التقنيات العلمية والمناهج قائمة على دراسة العالم المادي، حيث اعتادت الهيئات المكلفة بالتحقيق على الأدلة الملموسة، خلافا للعالم الافتراضي الذي تجد فيه هاته الأخيرة نفسها غير قادرة على تطبيق إجراءات الإثبات التقليدية على الجرائم المرتكبة في هذا العالم، وبدلا من ذلك يحتاج المحققون إلى خبرات تقنية متخصصة وتدريب(تكوين) من اجل البحث في الأدلة على غرار فحص الأقراص الصلبة ووسائل وأنظمة الكترونية أخرى.

Master 2/ criminal law

Text N°: 08

Elecronic Evidence and its authenticity in forensic evidence (2nd part)

As defined by the Council of Europe, “electronic evidence” means any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system or network.

In scientific sources, this definition is considered in a similar way. In a broad sense, electronic evidence is any evidential information stored electronically on any type of electronic device that can be used as evidence in a lawsuit.

The digital evidence is diverse and is rapidly improving. Electronic evidence varies in form and type and may include raw data, monitoring systems across networks and servers, or electronic documents and digital signatures, or audiovisual recordings or attachments stored in e-mail.

It is required for forensic evidence to be accepted as evidence if it is obtained legally. Investigators are required to collect evidence according to the policies and procedures set by law. If these policies and procedures are violated during the inspection of computer systems and evidence collection the inspection becomes null. It is not permissible to adhere to what is not in the violated inspection record, and the court cannot rely on it in its ruling. There are many legal trends concerning the validity of the electronic evidence. Opinions differ regarding the evidence upon which a judge bases their conviction. These legal trends can be divided into two main schools of thought: the free proof system, and the legal evidence system.

Unrestricted evidence and free proof system gives the judge the freedom to accept the facts presented without requiring them to rely on specific evidence when forming their convictions. They are free to build their convictions on any evidence, even if it was not stipulated. Besides, all evidence is equal for the legislator in the evidence, and the judge determines what they consider to be valid. In the free proof system, there is no problem regarding the legality of the existence of digital evidence, because the existence of the evidence proves its legitimacy.

According to legal evidence system the judge’s role is confined to examining the evidence and ensuring that the conditions set by law for the validity of the work are fulfilled.

Considering the issue of legitimacy of accessing digital evidence, it should be noted that the possibility of obtaining electronic evidence raises several legal challenges due to the special nature of such evidence. The source of the data, and the hardware that can be searched related to collecting evidence that requires the assistance of technical experts in this field, are just some of the challenges that arise when handling digital evidence.

The strength of the inferential authenticity of the outputs obtained from computer and information technology lies in the truthfulness of the attribution of the act to a specific person or its lie, or the value of the output generated from the computer in its multiple forms of electronic or paper outputs.

Specialists may encounter, when gathering evidence and after confirming its legitimacy, and the legitimacy of the procedure of obtaining it, other difficulties. These challenges are largely due to the technical nature of the electronic data, and from interference with the evidence. Non-specialists do not always have the ability to detect tampering, which affects the validity of the electronic data to the degree of certainty, and its adoption as forensic evidence in establishing the facts and reaching a conviction or innocence. Among the most prominent of these difficulties are the following:

Difficulties regarding the validity of digital evidence allowed before the courts are numerous. First, digital evidence can be manipulated to hide the truth, so it does not reflect the reality of the crime being investigated. This manipulation may affect in all other digital evidence presented before the judiciary, and it weakens its authenticity and taking it with certainty. The possibility of technical errors while obtaining the digital evidence is very rare, but it weakens the perception of the authenticity of the digital evidence. Making decisions using evidence whose validity is less than that usually required calls into question the validity of a court decision.

Legal terms :

Electronic evidence	الدليل الالكتروني
The authenticity	الحجية
forensic evidence	الدليل الجنائي(الشرعي)
evidential information	معلومات استدلالية (اثباتية)
Council of Europe	مجلس أوروبا
Lawsuit	الدعوى القضائية
digital evidence	الدليل الرقمي
Electronic documents	الوثائق (المستندات) الرقمية
digital signatures	التوقيع الالكتروني
Legally obtained	المحصل عليها بطريقة قانونية
Investigators	المحققون (جهات التحقيق)
Are requred	متطلبة (مشروطة)
policies and procedures set by law	الشروط والإجراءات القانونية

are violated	منتهكة
the inspection	التفتيش
Null	باطلة
is not permissible	لا يجوز(غير مسموح به)
Ruling	الحكم
Legal trends	الاتجاهات القانونية
the validity of the electronic evidence	صحة وسلامة الدليل الالكتروني
The judge bases	يؤسس القاضي
Their conviction	قناعاته
the free proof system	نظام الاثبات الحر
the legal evidence system	نظام الاثبات القانوني (المقيد)
Unrestricted evidence	الدليل الغير مقيد
The facts	الحقائق
The legislator	المشرع
The legality of the existence	مشروعية الوجود
proves its legitimacy	تثبت شرعيته
to examining the evidence	فحص الدليل
legitimacy of accessing digital evidence	شرعية تقدير الدليل الالكتروني
legal challenges	التحديات القانونية
Inferential authenticity	الحجية الاستدلالية
To detect tampering	كشف التلاعب
Forensic evidence	الدليل الجنائي
Conviction	الادانة
Innocence	البراءة
Allowed	المسموح به(ا)
The crime being invetigated	الجريمة محل التحقيق
Manipulation	االتلاعب
Judisciary	الجهة القضائية
Court decision	حكم المحكمة

الدليل الجنائي وحجيته في الإثبات الجنائي (الجزء الثاني)

يعرف مجلس أوروبا الدليل الالكتروني بأنه الدليل الذي تم الحصول عليه من بيانات موجودة في جهاز أو التي تم إنشاؤها بواسطة جهاز والتي يعتمد تشغيلها على البرامج أو البيانات المخزنة أو المحولة (المنقولة) عبر نظام الكمبيوتر أو نظام الشبكة.

وقد تبنت مختلف المصادر العلمية نفس التعريف، وفي معناه الأوسع يعني الدليل الالكتروني كل معلومات استدلالية مخزنة إلكترونيا في أي نوع من الأجهزة الالكترونية يمكن استخدامها كدليل في الدعوى القضائية.

تتعدد الأدلة الرقمية نوعا وشكلا، وتتطور بسرعة، ويمكن أن تشمل البيانات الخام، أنظمة التحكم(المراقبة) عبر الشبكات والخوادم، أو الوثائق والمستندات والتوقيعات الالكترونية، التسجيلات السمعية البصرية، أو المرفقات المخزنة في الايميلات.

ومن متطلبات(شروط) الأدلة الالكترونية حتى تقبل كأدلة إذا تم الحصول عليها بطريقة شرعية (قانونية) أن تجد جهات التحقيق نفسها ملزمة بجمع الأدلة حسب السياسات والإجراءات القانونية، وإذا ما تم مخالفة هذه السياسات والإجراءات أثناء تفتيش أنظمة الكمبيوتر وجمع الأدلة فإن التفتيش يصبح باطلا، ولا يجوز الالتزام بما هو غير موجود في محاضر التفتيش المخالفة ولا يمكن بأي حال من الأحوال للمحكمة الاعتماد عليها في حكمها.

هناك العديد من الاتجاهات القانونية التي تتعلق بصلاحية الدليل الالكتروني، كما تختلف الآراء المتعلقة بالأدلة التي يؤسس عليها القاضي قناعاته، وتنقسم هذه الاتجاهات القانونية الى مدرستين فكريتيتن أساسييتين هما: نظام الإثبات الحر ونظام الأدلة القانونية (الإثبات القانوني).

1 –نظام الأدلة الغير مقيدة: (نظام الإثبات الحر): ويعطي للقاضي الحرية في قبول الحقائق المقدمة (المعروضة) دون الحاجة إلى الاعتماد على أدلة محددة عند بناء قناعاته، فالقضاة أحرار في تأسيس قناعاتهم بناءا على أي دليل ما لم ينص على خلاف ذلك.

إضافة إلى كون كل الأدلة متساوية في الإثبات بالنسبة للمشرع، والقاضي هو من يحدد ما يمكن اعتباره شرعيا، وبالتالي لا توجد مشكلة في هذا النظام اتجاه شرعية وجود الأدلة الرقمية لان وجود الدليل يثبت شرعيته.

2- نظام الاثبات القانوني: وفيه يقتصر دور القضاة على فحص الأدلة وضمان توافر الشروط القانونية لإثبات صحة العمل، وبالنظر إلى مسألة شرعية الوصول إلى الأدلة الرقمية، تجدر الإشارة إلى أن إمكانية الحصول على الأدلة الالكترونية تثير العديد من التحديات القانونية بحسب الطبيعة الخاصة لهذه الأدلة التي مصدرها البيانات والأجهزة، من حيث البحث عنها وجمعها إضافة إلى أن التعامل مع هذا النوع من الأدلة يتطلب مساعدة الخبراء التقنيين في هذا المجال.

إن قوة الحجية الاستدلالية للنتائج المحصل عليها بواسطة الحاسوب وتكنولوجيا المعلومات تكمن في صحة إسناد الفعل إلى شخص معين أو عدم صحته، أو في قيمة النتيجة المحصل عليها من الكمبيوتر في كل أشكال نتائجه (مخرجاته) الالكترونية والورقية.

قد يواجه المتخصصون صعوبات أخرى أثناء وبعد جمع الأدلة والتأكد من شرعيتها ومشروعية إجراءات الحصول عليها وذلك راجع إلى الطبيعة التقنية للبيانات الرقمية وتداخلها مع الأدلة.

أما غير المتخصصين فليس بإمكانهم القدرة على اكتشاف التلاعب الذي يؤثر على صحة وسلامة البيانات الالكترونية إلى درجة اليقين، واعتمادها كدليل جنائي في إثبات الوقائع والوصول إلى الإدانة أو البراءة ومن هاته الصعوبات صعوبات تتعلق بصلاحية الدليل الالكتروني المسموح به أمام المحاكم والتي تتمثل في إمكانية التلاعب بالأدلة الرقمية لإخفاء الحقيقة، حيث لا تعكس الجريمة محل التحقيق حقيقة، ويمكن أن يؤثر هذا التلاعب على باقي الأدلة الرقمية المقدمة أمام القضاء مما يمكنه إضعاف حجيتها والأخذ بها على وجه اليقين.

إن إمكانية وقوع الأخطاء التقنية أثناء الحصول على الأدلة الرقمية أمر جد نادر، لكنه يضعف من تصور ومعرفة حجية الدليل الرقمي.

وفي النهاية فإن اتخاذ القرارات باستخدام الأدلة التي تكون حجيتها أقل من تلك المطلوبة عادة ما يدعو إلى التشكيك في صحة قرار المحكمة.

Master 2/ criminal law

Text N°: 09

Information Security in The Algerian Law (part 1)

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.

-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 follow:

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, 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 seven 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- **Crimes related to Internet activities**: Stipulated in the articles of Section seven 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	الحجية
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	جريمة تخريب البيانات واتلافها

data	
By cheat(to cheat)	عن طريق الغش(يغش)
Information fraud crime	جريمة الاحتيال المعلوماتي
Article 120 bis	المادة 120 مكرر
Disclosure	الافشاء، الافصاح
Unfair competition	المنافسة الغير مشروعة
Espionage	التجسس
Terrorism	الارهاب
Unlawfull acts	التصرفات الغير قانونية(الغير مشروعة)
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 lives	اعتداء على حرمة الحياة الخاصة
Permission or consent of the owner	اذن او رضا صاحبها

الأمن المعلوماتي (السيبيراني) في التشريع الجزائري

يعني الأمن المعلوماتي توفير الحماية للمعلومات من المخاطر التي تهددها او الحواجز التي تمنع سوء استعمالها وذلك بتوفير الوسائل والادوات والمعايير والاجراءات التي تتخذ لحماية المعلومة من الوصول إلى الأشخاص الغير مرخص لهم، ولضمان حجيتها 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 15/04المتضمن تعديل قانون العقوبات، والذي تكون حسبه بعض التصرفات المتعلقة بالمعالجة الالية للبيانات مجرمة، على غرار:

1-**جريمة الدخول الغير مرخص به**: وهي قائمة أساسا على النفاذ الغير مرخص به لنظام المعلومات، وقد تم الاشارة 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 عمل 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 بأنها(كل من ادخل عن طريق الغش بيانات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل عن طريق الغش المعطيات المحتواة في الفرع الخامس من قانون العقوبات، واقر عقوبة الحبس والغرامة لمرتكبها.

5-**الجرائم المتعلقة بنشاطات الانترنت**: والتي نص عليها في مواد القسم السابع مكرر من قانون العقوبات، خاصة المادة 394مكرر 2/2 " أعمال الحيازة والنشر التي تقع على البيانات الالكترونية بهدف المنافسة الغير مشروعة، التجسس، الإرهاب، التحريض على الفسوق، وكل التصرفات الغير شرعية"(و هو المعنى الأوسع 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 (العمومية).

أكثر من ذلك، فقد قرر التشريع الجزائري حماية الأشخاص 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/ criminal law

Text N°: 10

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 Procedures, has given local jurisdiction to the Procurator of the Republic in information crimes, stipulated the inspection in Article 45, And on arrest for consideration 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 special 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 a scientific activity, 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.

C) **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 the protection 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 Algeriers 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 with holding 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
Special 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 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).

2-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 7/45 منه، والتوقيف للنظر في جرائم الاعتداء على انظمة المعالجة بموجب المادة 6/51 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
3-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:

-**قوانين الملكية الصناعية**: حيث جسد المشرع ذلك بتنظيم أحكام العلامات التجارية في الأمر 06/03 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 .

-**قوانين الملكية الأدبية**: مع التطورات الملحوظة في مجال المعلوماتية، والتي مست مختلف وسائل نقل الإنتاج الفكري، وسع المشرع الجزائري من خلال الأمر 10/97 المعدل والمتمم بالأمر 05/03 من قائمة المنتجات المحمية، حيث دمج تطبيقات الوسائط ضمن المصنفات الأصلية المعبر عنها في أعمال 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 الأعمال المعلوماتية.

-**الأمن المعلوماتي في قانون مكافحة جرائم الإعلام وتكنولوجيا الاتصال** : يتضمن القانون 04/09 الصادر في الجزائر قواعد للوقاية والرقابة على الجرائم المتعلقة بالمعلومات وتكنولوجيا الاتصال، ويجيز بموجبه مراقبة المعلومات الالكترونية في الأمور المتعلقة بالإرهاب والمخالفة للنظام العام.

حيث يهدف هذا القانون لحماية أنظمة المعالجة الآلية للبيانات من الجرائم وتحديد نطاق التحريات، وبالرغم من سرية الاتصالات وجدية التهديدات المحتملة، وأهمية 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 الإرهاب، 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 الإذن لضباط الشرطة القضائية لمدة ستة اشهر قابلة للتمديد.

حيث نص هذا القانون في الفصل الثالث منه على القواعد الإجرائية الخاصة بعملية التفتيش في مجال الجرائم المتعلقة بالمعلومات وتكنولوجيا الاتصال وفقا للمعايير المطبقة عالميا، مع إمكانية اللجوء إلى مساعدة السلطات الأجنبية المختصة بهدف تفتيش(مراقبة) أنظمة المعلومات الموجودة في الخارج.

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

كما نص الفصل الخامس على إنشاء لجنة وطنية للوقاية من الجرائم المتعلقة بالمعلومات وتكنولوجيا الإعلام ومكافحتها والتي تتولى التنسيق والتفعيل من أجل منع الجرائم الالكترونية ومساعدة السلطات القضائية ومصالح الشرطة القضائية في تحقيقاتها اتجاه الجرائم المتعلقة بالإعلام حسب نص المادة 14 من نفس القانون، كما يعود الاختصاص القضائي للمحاكم الجزائرية إذا ما تم ارتكاب هذه الجرائم خارج الإقليم الجزائري عندما يكون الفاعلون أجانب ويستهدفون مؤسسات الدولة، وهنا تكون المساعدة القضائية مطلوبة بشرط ان لا تنتهك السيادة.

Master 2/ criminal law

Text N°: 11

Challenges to international cooperation to fight transnational cybercrime

The ever growing use of computer and information communication technologies in the world has opened up a range of new activities for crime to take place through electronic means on a global scale, irrespective of national and transnational borders.

The effective combating , investigation and prosecution of such crimes require international cooperation between countries, law inforcement agencies and instituttions backed by laws, international relations, conventions, directives and recommendations culminating in a set of international guidelines to fight cybercrime. Challenges to international cooperation and establishing international guidelines to fight global cybercrime across borders are :

1 – **lack of harmonization of national criminal laws reguarding to cybercrimes** and the difficulties to find a clear and a comprehensive definition of computer related crime , therehas been a great debate among experts regarding what constitutes a cybercrime.

Intent of different authors to be precise about the scope and use of particular definitions means , however, that the use of these definitions out of their intended context often creates inaccuracies, with a result that a universally agreed definition of computer crime has not been achieved to date.

2-**the extent of cybercrime** : while it is possible to give an accurate description of computer offences committed, it has prooved difficult to give an accurate overview of the extent of losses and the actual number of cybercriminal acts. Crimes statistics do not represent the real number of offences.

3- **difficulties of locating and identifying perpetrators across borders** : cybercrime is infinitely more difficult to presecute than physical crimes.the nature of the internet with its far- reaching links and easy anonymity , offers the opportunity for perperators to launch attacks and disappear quickly. In addition of requiring cooperation between countries in identifying perpetrators of serious offences of international scope, cooperation is also required for all available resources including law enforcement,military and intelligence agencies.

4-**computer procedural problems** : the legal world has been based on paper for so long that adaptation to the digital era has processed slowly in relation to the digitization of the rest of the business world, in the law few years courts have begun routinely to accept electronic evidence, though always very carefully, frequently, discussions about electronic evidence become a confrontation among forensic technologists. The replacement of visible and coporeal objects of proof with invisible and intangible evidences in the field of information technology not only creates practical problems but also opens up new legal issues; the

coercive powers of prosecuting authorities, specific problems with personal data and admissibility of computer-generated evidence.

5-**conflicts of jurisdiction** :there are also a number of complex jurisdictional issues to confront, given the multiplicity of countries potentially involved in a cybercrime. How can it be determined in which country the crime was actually committed ? or who should have jurisdiction to perscribe rules of conduct or of adjudication ?

summing up :

law inforcement tipically stops at the borders of nation states and must go through proper leagal channels and procedures to receive assistance in pursuing cybercrime investigations and prosecutions, it also becomes neceesary to seek the assistance aand support of agencies such as interpol…ect.to not only help the invesigations and prosecution processes but also in extradition of criminals from one jurisdiction to an other. These processes require a complex of differnt skill levels for cybercrime investigations, forensic analyses, custody of the evidence, prosecution and extradition within a country, between countries and agencies to be efficient and effective.

Legal terms :

International cooperation	التعاون الدولي
National and transnational borders	الحدود الوطنية والعبروطنية
Investigation and prosecution	التحقيق والمتابعة القضائية
Law enforcement agencies and institutions	هيئات ومؤسسات انفاذ القانون
International relations	العلاقات الدولية
Conventions	الاتفاقيات
Directives	التوجيهات
Recommendations	التوصيات
International guidelines	المبادئ الارشادية الدولية
To fight cybercrime	محاربة الجريمة السيبيرانية
National criminal laws	القوانين الجنائية الوطنية
Cybercriminal acts	التصرفات السيبيرانية الاجرامية
Perpertators	المجرمون (الفاعلون)
To prosecute	تابع قضائيا
Physical crimes	الجرائم المادية

Offences of international scope	الجرائم العالمية النطاق
Law enforcement, military agencies	هيئات انفاذ القانون، والهيئات العسكرية
Digitization	الرقمنة
invisible and intangible evidences	الادلة الغير مرئية والغير ملموسة
Legal issues	القضايا (المسائل القانونية)
coercive powers of prosecuting authorities	القوة القسرية لسطات المقاضاة
admissibility of computer-generated evidence	مقبولية الأدلة الالكترونية
Conflicts of jurisdiction	تنازع الاختصاص القضائي
jurisdictional issues	قضايا الاختصاص القضائي
rules of conduct	قواعد السلوك
Rules of adjudication	قواعد التحكيم
legal channels and procedures	قنوات واجراءات قانونية
Law enforcement	إنفاذ القانون
Assistance in pursuing	المساعدة في المتابعة
Cybercrime investigations and prosecutions	التحريات والمتابعة القضائية للجرائم الاكترونية
The extradition of criminals	تسليم المجرمين
investigations and prosecutions processes	عمليات التحري والمتابعة القضائية
custody of the evidence	الرقابة على الأدلة

تحديات التعاون الدولي في محاربة الجرائم السيبيرانية العابرة للحدود

ان الاستعمال المتزايد للحاسوب وتكنولوجيا المعلومات والاتصال في العالم قد فتح المجال لمجموعة من النشاطات الجديدة لوقوع الجرائم من خلال الوسائل الالكترونية على نطاق عالمي، متجاهلة بذاك للحدود الوطنية والعبر وطنية.

تتطلب المكافحة الفعالة لهذه الجرائم والتحري والمتابعة فيها تعاونا دوليا بين الدول، وهيئات ومؤسسات إنفاذ القانون المدعومة بالقانون، العلاقات الدولية، الاتفاقيات، التوجيهات، والتوصيات التي بلغت ذروتها في مجموعة من القواعد الإرشادية الدولية لمحاربة الجريمة السيبيرانية.

تكمن تحديات التعاون الدولي ووضع مبادئ إرشادية دولية لمحاربة الجرائم السيبيرانية العابرة للحدود فيما يلي:

1-**غياب تناسق للقوانين الوطنية الجنائية اتجاه الجرائم السيبيرانية** والصعوبات في إيجاد تعريف واضح ومفهوم للجرائم المتعلقة بالحاسوب، فالنقاش كبير بين الخبراء حول ما يشكل أو يكون جريمة سيبيرانية.

كما أن نية الفقهاء مختلفة في ان يكونوا دقيقين بشأن نطاق واستعمال وسائل وتعاريف معينة، ومع ذلك فإن استخدام هذه التعاريف يكون خارج السياق المقصود وعادة ما يخلق حالات من عدم الدقة ما يعني عدم وجود تعريف متفق عليه عالميا لحد الآن.

2- **امتداد الجريمة الالكترونية**: رغم أنه عاد بالإمكان إعطاء وصف دقيق للجرائم المرتكبة بالكومبيوتر، فقد ثبتت صعوبة إعطاء نظرة دقيقة أو رأي حول مدى الخسائر وحول العدد الفعلي للتصرفات الاجرامية السيبيرانية، فإحصائيات الجرائم لا تمثل رقما حقيقيا حول الجرائم.

3-**صعوبات تحديد موقع المجرمين عبر الحدود**: فالجريمة السيبيرانية صعبة من حيث المقاضاة مقارنة بالجرائم المادية، بحكم طبيعة الانترنت والروابط التي من الصعب الوصول اليها، ناهيك عن المجهولية السهلة المتاحة عبرها حيث تمنح الفاعلين إمكانية الاعتداء(التعدي) والاختفاء بسرعة، بالإضافة الى التعاون المطلوب بين الدول لتحديد المجرمين او مرتكبي الجرائم الخطيرة ذات النطاق الدولي، كما أنه مطلوب أيضا بالنسبة لكل الموارد المتاحة بما فيها هيئات إنفاذ القانون والهيئات العسكرية، وهيئات الذكاء.

4-**المشاكل الاجرائية للكمبيوتر**: يقوم العالم القانوني منذ القدم على الورق، إلا أن تبني الحقبة الرقمية والذي ثبت معالجته ببطء فيما يتعلق بالرقمنة في عالم الاعمال، إلا أن الملاحظ أنه في السنوات الاخيرة بدأت المحاكم تقبل الادلة الالكترونية بشكل روتيني بالرغم من الحذر الشديد، حتى أن النقاشات حول الادلة الالكترونية أصبحت تخلق مواجهات بين علماء التكنولوجيا العلمية. كما ان استبدال الادلة المرئية والاشياء المادية في الاثبات بأدلة غير ملموسة وغير مرئية في مجال تكنولوجيا المعلومات لا يخلق فقط مشاكل عملية، بل يفتح المجال أمام قضايا قانونية جديدة مثل الاكراه(القوة القسرية) لسلطات المقاضاة ومسائل خاصة بالنسبة البيانات(المعطيات) الشخصية ومقبولية الدليل الالكتروني المنشأ بواسطة الكمبيوتر.

5- **تنازع الاختصاص**: هناك العديد من المسائل المتعلقة بالاختصاص القضائي المعقد والواجب مواجهتها، فرغم تعدد الدول المحتمل أن تشملها الجريمة السيبيرانية يمكن التساؤل حول كيفية تحديد الدولة التي ارتكبت فيها الجريمة فعلا؟ أو من يكون له الاختصاص في تحديد قواعد السلوك أو التحكيم؟

خلاصة:

عادة ما يتوقف إنفاذ القانون على حدود الدول، والذي يجب أن يتم عبر قنوات وإجراءات قانونية خاصة لتلقي المساعدة في متابعة التحريات ومقاضاة الجرائم السيبيرانية، ويصبح البحث ضروريا عن المساعدة والدعم من مختلف الهيئات مثل الانتربول....الخ، وهذه الاخيرة لا تنصب على التحقيقات والمتابعة القضائية فقط بل تتعداها الى تسليم المجرمين بين الجهات القضائية المختصة.

إن هذه العمليات تتطلب مجموعة معقدة من مختلف مستويات صلاحيات التحري في الجرائم الالكترونية والتحليل الشرعي لها وفي رقابة الاثبات والمتابعة االقضائية وتسليم المجرمين داخل الدولة وبين الدول والهيئات حتى تكون كافية وفعالة.